明らかである。

【００２７】請求項の記載に関連して本発明はさらに次の態様をとりうる。

【００２８】（１）前記指令送出手段は、自装置の電源投入時に前記識別情報送出指令を送出することを特徴とする請求項１又は２記載の記憶装置。

【００２９】（２）前記指令送出手段は、自装置のイニシャライズ時に前記識別情報送出指令を送出することを特徴とする請求項１又は２記載の記憶装置。

【００３０】（３）前記指令送出手段は、前記記憶装置の電源投入時に前記識別情報送出指令を送出することを特徴とする請求項３記載の機密保持システム。

【００３１】（４）前記指令送出手段は、前記記憶装置のイニシャライズ時に前記識別情報送出指令を送出することを特徴とする請求項３記載の機密保持システム。

【００３２】

【発明の効果】以上説明したように本発明は、識別情報指令に応答して外部アクセス装置から入力された識別情報と記憶装置の識別情報とが一致したときにのみデータのアクセスを許可し、また識別情報指令の送出時から所定時間内にアクセス装置から識別情報の入力があったときにのみデータのアクセスを許可することにより、記憶装置に保持されたデータの機密を保持することができるという効果がある。

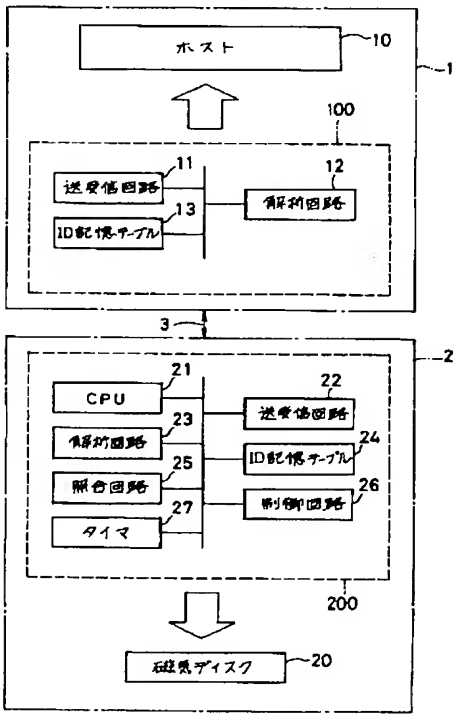
【図面の簡単な説明】

【図１】本発明の実施例による機密保持システムの構成を示すブロック図である。

【符号の説明】

１　ホスト
２　磁気ディスク装置
３　通信経路
１０　ホスト機構
２０　磁気ディスク機構
１１、２２　送受信回路
１２、２３　解析回路
１３、２４　ＩＤ記憶テーブル
２１　ＣＰＵ
２５　照合回路
２６　制御回路
２７　タイマ
１００、２００　機密保持機構

【図１】



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-293936
(43)Date of publication of application : 20.10.2000

(51)Int.Cl. G11B 20/10
G11B 20/12
H04N 5/91
H04N 5/92

(21)Application number : 11-100976
(22)Date of filing : 08.04.1999

(71)Applicant : HITACHI LTD
(72)Inventor : SASAMOTO MANABU
OKAMOTO HIROO
CHIBA HIROSHI
OWASHI HITOAKI

(54) DIGITAL SIGNAL RECORDER, REPRODUCING DEVICE AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a recorder, reproducing device and recording medium, capable of protecting the copyright of a digital signal on the recording medium.
SOLUTION: In the digital signal recorder, reproducing device and recording medium for recording or reproducing the digital signal on the recording medium, the digital signal is enciphered by a key obtained in the manner of executing the specific calculation to the key information at the time of recording and recorded to the recording medium together with the key information. At the time of reproduction, the reproduced digital signal is deciphered and outputted by the key obtained in the manner of executing the specific calculation to the key information reproduced from the recording medium.

LEGAL STATUS

[Date of request for examination] 04.09.2003
[Date of sending the examiner's decision of rejection] 26.09.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] In the digital signal recording device which records a digital signal on a record medium A key information generating means to generate at least one key information, and a key generating means for said key information to be inputted, to perform a predetermined operation, and to generate a key, A code conversion means for said key and said digital signal to be inputted, and to encipher and output said digital signal with said key, and said at least one key information, with said enciphered digital signal The digital signal recording device characterized by having a record means to record on the predetermined field on said record medium.
[Claim 2] Said digital signal is a digital signal recording device according to claim 1 characterized by coming to have the packet format of predetermined length.
[Claim 3] It is the digital signal recording device according to claim 1 characterized by having equipped said key information generating means with the function which updates said at least one key information with the predetermined time interval, and equipping said record means with the function which records identifiable information for the timing to which said key information generating means updates said key information on the predetermined field on said record medium.
[Claim 4] It is the digital signal recording device according to claim 3 which said digital signal comes to have the packet format of predetermined length, and is characterized by equipping said record means with the function which adds identifiable information to each packet of said digital signal, and records the timing to which said key

information generating means updates said key information on said record medium.
[Claim 5] It is the digital signal recording device according to claim 1 which said code conversion means is equipped with the function which can choose further the function which enciphers and outputs said digital signal, and the function which output as it is without enciphering, and said record means records the code flag information which shows whether said digital signal is enciphered on the predetermined field on said record medium, and characterizes by to have had the function which does not record said key information when not enciphering.
[Claim 6] It is the digital signal recording device according to claim 5 which said digital signal comes to have the packet format of predetermined length, and is characterized by equipping said record means with the function which adds the code flag information which shows whether said digital signal is enciphered to each packet of said digital signal, and records it on said record medium.
[Claim 7] Input the digital signal of predetermined length, add a synchronizing signal and a management information signal, and it considers as a sector format. Add the 1st error correcting code to said sector, and the 2nd error correcting code is further added per n (n is one or more integers) sector. In the digital signal recording device which adds the 1st error correcting code also to said 2nd error correcting code, and is recorded on a record medium A key information generating means to generate at least one key information, and a key generating means for said key information to be inputted, to perform a predetermined operation, and to generate a key, A code conversion means for said key and said digital signal to be inputted, and to encipher and output said digital signal with said key, and said at least one key information, with said enciphered digital signal The digital signal recording device characterized by having a record means to record on the predetermined field on said record medium.
[Claim 8] Said key information generating means has the function which updates said at least one key information at intervals of predetermined time. Said key generating means Said updated key information is inputted at least, and the key updated by performing said predetermined operation is generated. Said code conversion means The digital signal recording device according to claim 7 characterized by having the function switched to said updated key by the break eye of the unit of n sector which added said 2nd error correcting code.
[Claim 9] Said code conversion means has the function which can choose the function which enciphers and outputs said digital signal, and the function outputted as it is without enciphering. Said record means By the break eye of the unit of the sector which recorded the code flag information which shows whether said digital signal is enciphered on the predetermined field on said record medium, and added said 2nd error correcting code The digital signal recording device according to claim 7 characterized by having the function which switches whether said digital signal is enciphered.
[Claim 10] In the digital signal regenerative apparatus which reproduces the digital

signal currently recorded on the record medium At least one key information currently recorded on the predetermined field on said record medium, A playback means to reproduce said digital signal, and a key generating means for said key information to be inputted, to perform a predetermined operation, and to generate a key, The digital signal regenerative apparatus characterized by having a decode conversion means for said key and said reproduced digital signal to be inputted, and to decrypt and output said digital signal with said key.

[Claim 11] Said digital signal is a digital signal regenerative apparatus according to claim 10 characterized by coming to have the packet format of predetermined length.

[Claim 12] It is the digital signal regenerative apparatus according to claim 10 characterized by having the function to have a key information generating means to generate other at least one key information, and for said key information, and key information besides the above to be inputted, and for said key generating means to perform a predetermined operation, and to generate a key.

[Claim 13] Said key information by which the place where said playback means is recorded on the predetermined field on said record medium was updated, It has the function which reproduces identifiable information for the timing which updates said key information. Said key generating means Said updated key information is inputted at least, and it has the function to generate the key updated by performing a predetermined operation. Said decode conversion means The digital signal regenerative apparatus according to claim 10 characterized by having the means which sets said inputted key by said timing signal, and switches it to said updated key.

[Claim 14] It is the digital signal regenerative apparatus according to claim 13 which said digital signal comes to have the packet format of predetermined length, and is characterized by equipping said playback means with the function which reproduces identifiable information for said timing currently added and recorded on each packet of said digital signal.

[Claim 15] Said playback means is equipped with the function which reproduces the code flag information which shows whether said digital signal currently recorded on the predetermined field on said record medium is enciphered. Said decode conversion means using said code flag information The digital signal regenerative apparatus according to claim 10 characterized by having the function which chooses and switches the function which decrypts and outputs said reproduced digital signal, and the function outputted as it is without decrypting.

[Claim 16] It is the digital signal regenerative apparatus according to claim 15 which said digital signal comes to have the packet format of predetermined length, and is characterized by equipping said playback means with the function which reproduces the code flag information which shows whether said digital signal currently added and recorded on each packet of said digital signal is enciphered.

[Claim 17] Add a synchronizing signal and a management information signal to the digital signal of predetermined length, and it considers as a sector format. Add the 1st

error correcting code to said sector, add the 2nd error correcting code per n (n is one or more integers) sector further, and the 1st error correcting code is added also to said 2nd error correcting code. In the digital signal regenerative apparatus which reproduces said digital signal currently recorded on the record medium At least one key information currently recorded on the predetermined field on said record medium, A playback means to reproduce said digital signal, and a key generating means for said key information to be inputted, to perform a predetermined operation, and to generate a key, The digital signal regenerative apparatus characterized by having a decode conversion means for said key and said reproduced digital signal to be inputted, and to decrypt and output said digital signal with said key.

[Claim 18] It is the digital signal regenerative apparatus according to claim 17 characterized by having the function to have a key information generating means to generate other at least one key information, and for said key information, and key information besides the above to be inputted, and for said key generating means to perform a predetermined operation, and to generate a key.

[Claim 19] Said playback means is equipped with the function which reproduces said key information by which the place currently recorded on the predetermined field on said record medium was updated. Said key generating means It is the digital signal regenerative apparatus according to claim 17 characterized by having inputted said updated key information at least, having had the function to generate the key updated by performing a predetermined operation, and equipping said decode conversion means with the means which switches said inputted key to said updated key.

[Claim 20] Said playback means is a digital signal regenerative apparatus according to claim 19 characterized by having the function which reproduces said key information updated by the break eye of the unit of n sector which added said 2nd error correcting code.

[Claim 21] It is the digital signal regenerative apparatus according to claim 17 which carries out [that equipped said playback means with the function which reproduces the code flag information which shows whether said digital signal currently recorded on the predetermined field on said record medium is enciphered, and said decode conversion means had the function which chooses and switches the function which decrypts and outputs said reproduced digital signal using said code flag information, and the function which output as it is without decrypting, and] as the description.

[Claim 22] Said playback means is a digital signal regenerative apparatus according to claim 21 characterized by having the function which reproduces said code flag switched by the break eye of the unit of n sector which added said 2nd error correcting code.

[Claim 23] The digital signal record medium with which said key information is characterized by what is recorded on the predetermined field with said digital signal enciphered with the key obtained by carrying out a predetermined operation to key information in the digital signal record medium with which the digital signal is recorded.

[Claim 24] Said digital signal is a digital signal record medium according to claim 23 characterized by coming to have the packet format of predetermined length.
[Claim 25] The digital signal record medium according to claim 23 characterized by updating said key information at intervals of predetermined, and recording it on the predetermined field.
[Claim 26] The digital signal recording device characterized by coming to have a key generating means to generate two or more kinds of keys for changing a digital signal, a conversion means to change a digital signal using said key and to output the conversion digital signal after conversion, and a record means to record said key and said conversion digital signal on a record medium.
[Claim 27] The digital signal regenerative apparatus [claim 28] which it comes to have in a playback means the medium by which the conversion digital signal changed with two or more kinds of keys and said key were recorded is used, reproduces said conversion digital signal and said key from said medium, and output, and the decode conversion means which the output from said playback means is inputted and carries out decode conversion of said conversion digital signal using said key The record medium with which the conversion digital signal changed with two or more kinds of keys and said key were recorded.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the digital signal recording apparatus which has the function to protect the copyright of the digital signal on a record medium especially, a regenerative apparatus, and a record medium about the digital signal recording apparatus which carries out record playback of the digital signal at a record medium, a regenerative apparatus, and a record medium.
[0002]
[Description of the Prior Art] Research of data compressions, such as an image, voice, etc. using a digital technique, progresses, and it came to be able to perform are recording of these data, and transmission easily in recent years. In connection with this, digitization is quickly advanced also in the field of broadcast.
[0003] For example, digital compression coding of an analog video signal and the sound signal is carried out at high efficiency using MPEG (Moving Picture Experts Group) specification, and the system broadcast through a satellite or a coaxial cable is known. As equipment for receiving this digital broadcast, there is a digital broadcast receiver called a set top box.

[0004] Moreover, development of the digital video tape recorder which records the video signal and sound signals by which digital compression coding was carried out, such as digital TV broadcast, with a digital signal, and can be reproduced is furthered, using a magnetic tape as a video signal for home use and a sound signal record playback device.
[0005] It connects with a digital interface and preservation of this digital broadcast receiver and digital video tape recorder is attained for high quality in the received digital broadcast.
[0006] Furthermore, development of the equipment which records a video signal and a sound signal and is reproduced is furthered using the optical disk or the hard disk.
[0007] The technique which receives the digital signal with which multiplex [of two or more information] is carried out, and it is transmitted, and chooses a desired program is expressed to Japanese JP,8-56350,A. Moreover, the digital video tape recorder using a rotating magnetic head is indicated by Japanese JP,5-174496,A, for example.
[0008] furthermore, about the digital broadcast record system which connected the digital video tape recorder with the digital broadcast receiver with a digital interface IEEE Tolan ZAKUSHONSU ON Consumer Electronics, Volume [42nd] No. 3, August, 1996, 617-622 pages () [IEEE Transactions] on Consumer Electronics and Vol. 42, No.3, August 1996, and p617-622 "Newly Developed D-VHS Digital Tape Recording System for the Multimedia Era" -- detailed -- stating -- ********.
[0009]
[Problem(s) to be Solved by the Invention] However, about defense of the copyright of the digital signal on a record medium which recorded digital broadcast etc. with the digital video tape recorder etc., it is not taken into consideration at all.
[0010] The object of this invention is to protect the copyright of the digital signal on a record medium.
[0011]
[Means for Solving the Problem] It is the key obtained by performing a predetermined operation to key information at the time of record in the digital signal recording device, the regenerative apparatus, and the record medium which records or reproduces a digital signal on a record medium, enciphers a digital signal, and this invention records on a record medium, and it is the key obtained by performing said predetermined operation, and it decrypts and outputs the digital signal which reproduced at the time of playback with said key information to said key information which reproduced from a record medium.
[0012]
[Embodiment of the Invention] Hereafter, the example of this invention is explained using a drawing.
[0013] Drawing 1 is a block diagram containing a digital broadcast receiver and a digital signal record regenerative apparatus. For 200, as for a digital broadcast receiving set and 202, a digital signal record regenerative apparatus and 201 are [an

antenna and 207] receiving sets. Moreover, as for 203, as for a tuner and 204, a selection circuitry and 205 are control circuits where a decoder circuit and 206 perform an interface circuitry and 208 controls actuation of the digital broadcast receiver 201. Here, although the digital broadcast receiver 201 and the digital signal record regenerative apparatus 200 are expressed as the configuration of another object, they may have composition of one.

[0014] Drawing 2 is the block diagram of the digital signal record regenerative apparatus 200 of drawing 1 . Although it is equipment of record playback combination, even if record and playback are in drawing 2 independently, it is the same. The record digital disposal circuit to which 100 performs a rotary head and, as for 101, a capstan and 102a perform generation of the record signal at the time of record etc., The regenerative-signal processing circuit where 102b performs the recovery of the regenerative signal at the time of playback etc., and 104 control a record playback mode etc. For example, a control circuit like a microprocessor, the timing generation circuit which generates the timing signal with which 105 becomes criteria, such as a revolution of a rotary head 100, The servo circuit where 106 controls the feed rate of a rotary head and a tape, the I/O circuit where 107 performs the input of a record signal, or the output of a regenerative signal, The timing-control circuit where 109 controls the timing at the time of record, the oscillator circuit where 110 generates a reference clock, In 111, a tape and 112 the data code circuit at the time of digital signal record, and 116 for the record regenerative circuit of an analog video signal, and 115 the data decoder circuit at the time of digital signal playback and 117 The device key generator which generates the device key which is the basis of the data key which supplies digital information to the data code circuit 115 or the data decoder circuit 116 a code or in case it decodes, The block key generator which generates the block key whose 118 is another basis of a code or the data key at the time of decoding about digital information, and 119 are input/output control circuits which perform the output control of the time stump processing to the packet data at the time of record, and the packet data at the time of playback.

[0015] A digital image compression signal is data of a packet format, and Time Division Multiplexing of the signal of two or more channels is carried out, and it is transmitted. In drawing 1 , it restores to the digital broadcast signal received with the antenna 202 with a tuner 203, and a required digital compression video signal is chosen by the selection circuitry 204 after that. The selected digital compression video signal is decoded by the video signal usual by the decoder circuit 205, and is outputted to a receiving set 207. Moreover, decode processing is performed after canceling it in a selection circuitry 204, when processing of a scramble etc. is performed to the input signal. When recording the received digital broadcast signal, the information relevant to the digital compression video signal and it which are recorded in a selection circuitry 204 is chosen, and it is inputted and recorded on the digital signal recording device 200 from the input/output terminal 108 of the digital

signal record regenerative apparatus 200 through an interface circuitry 206. Moreover, when reproducing the recorded digital broadcast signal, the digital compression video signal reproduced with the digital signal record regenerative apparatus 200 is outputted to an interface circuitry 206 from an input/output terminal 108. By the selection circuitry 204 and the decoder circuit 205, the digital compression video signal inputted into the interface circuitry 206 performs the same processing as the time of the usual reception, and outputs it to a receiving set 207.

[0016] In drawing 2 which shows the configuration of the digital signal record regenerative apparatus 200 of drawing 1 , some packet data inputted from the input/output terminal 108 are inputted into a control circuit 104 through the I/O circuit 107 at the time of record. In a control circuit 104, the information sent apart from the information or packet data added to packet data detects the class of packet data etc., by the detection result, a recording mode is judged and the mode of operation of record digital-disposal-circuit 102a and the servo circuit 106 is set up. Next, the I/O circuit 107 outputs the packet data to record to the data code circuit 115. In the data code circuit 115, with the data key generated in a control circuit 104 based on the key generated by the device key generator 117 and the block key generator 118, the inputted packet data are enciphered and this is outputted to the input/output control circuit 119. In the input/output control circuit 119, a time stump is given to the inputted packet data based on the hour entry from the timing generation circuit 105, and this is outputted to record digital-disposal-circuit 102a. In record digital-disposal-circuit 102a, according to the recording mode judged in the control circuit 104, record data including an error correcting code, ID information, a sub-code, the block key information used for encryption are generated, and a record signal is generated, and it records on a tape 111 by the rotary head 100.

[0017] At the time of playback, playback actuation is first performed by the playback mode of arbitration, and ID information is detected by regenerative-signal processing circuit 102b. And it judges in which mode it was recorded in the control circuit 104, and reproduces by resetting the mode of operation of regenerative-signal processing circuit 102b and the servo circuit 106. In regenerative-signal processing circuit 102b, from the regenerative signal reproduced from the rotary head 100, detection of a synchronizing signal, error detection correction, block key information, etc. are acquired, packet data are reproduced, and it outputs to the input/output control circuit 119. In the input/output control circuit 119, the packet data which removed the time stump on the basis of the timing generated in the timing generation circuit 105 are outputted to the data decoder circuit 116. In the data decoder circuit 116, it decodes with the data key generated in a control circuit 104 based on the key generated by the device key generator 117 and the block key obtained by playback, and outputs to it in the I/O circuit 107.

[0018] At the time of record, the timing of a record regenerative apparatus of operation is controlled by the timing-control circuit 109 on the basis of the rate of

the record data inputted from the input/output terminal 108, and it operates considering the clock oscillated by the oscillator circuit 110 as criteria of operation at the time of playback.

[0019] Drawing 3 is the block diagram of the packet of a digital image compression signal. One packet consists of fixed lengths, for example, 188 bytes, and is constituted by 4 bytes of packet header 306, and 184 bytes of packet information 307. A digital compression video signal is arranged to the field of the packet information 307. Moreover, a packet header 307 is constituted by information, such as a class of packet information.

[0020] Drawing 4 is the block diagram of the packet header 306 of drawing 3 . The scramble control whose synchronous cutting tool whom 501 shows the head of a packet, error indication 502 indicates the existence of an error to be, unit start identification 503 indicates initiation of a unit to be, packet priority 504 indicates the significance of a packet to be, packet ID 505 indicates the class of packet to be, and 506 show the existence of a scramble, the Adaptation field control 507 indicates the existence of additional information and the existence of packet information to be, and 508 are patrol counters counted up per packet.

[0021] Drawing 5 is the block diagram of the signal chosen from the transmission signal and transmission signal of digital broadcast. 71 is the packet of drawing 3 . Usually, a sound signal, the information about a program, etc. are added to the above-mentioned video signal, Time Division Multiplexing of the program of two or more channels is carried out, and it is transmitted.

[0022] Drawing 5 (a) is the example which carried out multiplex [of the program of three channels], and the video signal of each channel, A1 and A2, and A3 of V1, V2, and V3 are the packets of the sound signal of each channel. In addition, an image or voice may be constituted from two or more images or voice by one channel. P0, P1, P2, and P3 are the information about a program. A different packet ID 505 is assigned and, thereby, each packet can identify the content of the packet.

[0023] P0 is the information about the whole transmission signal of drawing 5 (a), and Time Division Multiplexing of the packets, such as a program association table for recognizing which packet ID is assigned and program guide information, is carried out to each program, and it is transmitted to it. P1, P2, and P3 are the information about each program, and Time Division Multiplexing of the packets, such as a programmed map table for recognizing which packet ID is assigned to the image packet of the channel, the packetized voice, etc. and scramble information, is carried out, and they are transmitted. Usually, the value it was decided that the packet ID of a program association table would be, 0 [for example,], is assigned.

[0024] At the time of reception, it recognizes which packet ID is assigned to the image packet, the packetized voice, etc. on the programmed map table of a program to recognize which packet ID is assigned to the programmed map table of a program to receive by the program association table first, next receive. And an image packet

and a packetized voice are extracted and digital compressed data is decoded. Moreover, a program clock reference is extracted simultaneously, and actuation of a decoder circuit is controlled so that the decode timing of the decoder circuit of digital compressed data synchronizes with the timing at the time of coding by this.
[0025] CR is a program clock reference source for taking the synchronization at the time of decode of digital compressed data.
[0026] Of course, four channels except three channels are sufficient as the number of channels which carries out multiplex, and it may carry out multiplex [of the information other than this].
[0027] Drawing 5 (b) chooses only the information on the 1st channel, and the program information relevant to it from drawing 5 (a). In recording the 1st channel, it outputs this information to the record regenerative apparatus 200 from the digital broadcast receiver 201. Of course, you may record including information other than this, and in order to make processing at the time of playback easy to do, a part of information on a packet may be changed. For example, if it changes into the information only on the program which records the information on a program association table, selection of a channel will become unnecessary at the time of playback.
[0028] Drawing 6 is the block diagram of the data code circuit 115 of drawing 2 . 1151 -- a packet data input terminal and 1157 -- a packet data output terminal, and 1153a and 1153b -- a data key input terminal and 1153c -- for a block processing circuit and 1154, as for a code machine, and 1158a and 1158b, a key schedule circuit and 1155 are [a processing-mode selection-signal input terminal, and 1152 and 1156 / a data key selection-signal input terminal and 1153d / a data key register and 1159] data key selectors. The data code circuit 115 is enciphered and outputted by the packet data unit inputted with the data key defined beforehand. Under the present circumstances, the safety of the packet data recorded on a tape can be raised by changing this data key with a certain time interval.
[0029] Even if the error of a bit error etc. occurs for example, during transmission, the block cipher which can realize cipher processing by easy circuitry by making into a unit the block which consists of two or more bits is used for the code machine 1155 so that the data of consecutiveness of the error may not be affected, namely, there may be no error propagation in them.
[0030] The packet data inputted from the input terminal 1151 are first divided into the block P which consists of two or more bits in the block processing circuit 1152. For example, 1 block is made into 64 bits. Sequential encryption is carried out in the code machine 1155, and, as a result, each block outputs Block C, in the block processing circuit 1156, shortly, returns a block to the format of packet data, and outputs it to an output terminal 1157. Here, from a control circuit 104, the data key which is a key for encryption is inputted from the data key input terminals 1153a and 1153b, and is memorized by the data key registers 1158a and 1158b. For example, the data key

which switches the present data key to data key register 1158b at a degree is made to record on data key register 1158a.
[0031] Moreover, from data key selection-signal input terminal 1153c, from a control circuit 104, the signal which shows which data key of the data key registers 1158a and 1158b is chosen is inputted, and the data key chosen by the data key selector 1159 is outputted. Here, the data key of key register 1158a shall be chosen, for example. The selected data key is changed into the sub keys KA and KB in the schedule circuit 1154, and is supplied to the code machine 1155. For example, die length of 56 bits of a data key and the die length of a sub key consider as 32 bits, respectively, assign 32 bits of high orders of a data key to KA, and assign the aggregate value of 32 bits of high orders of a data key, and 32 bits of low order to KB.
[0032] Here, from a control circuit 104, when changing a data key, a signal is inputted from data key selection-signal input terminal 1153c so that data key register 1158b may be outputted. A data key selector is controlled not to switch the selection output but to switch between the following packet data until encryption of all blocks of one packet data is completed.
[0033] In addition to this, an exclusive OR is taken for the output of the code machine 1155, and the input of the code machine 1155, and there is also the approach of increasing code reinforcement by applying feedback per block.
[0034] Drawing 7 is the block diagram of the code machine 1155 of drawing 6 . The cipher-processing section, the data with which Pa was enciphered for 551, 552, 553, and 554 among this drawing, and the high order of the input block data P and a lower bit, and calcium and Cb were enciphered for Pb, and KA and KB are sub keys. As shown in this drawing, the inputted 64-bit block P is divided into Pb 32 bits of the high order Pa, and 32 bits of low order. It sets in the cipher-processing section 551, and the Pa and Pb are an exclusive OR (5511), a bit shift, and an add operation (5512, 5513, and 5515:A<<<p). The add operation (5514 5516) showing carrying out the circulation bit shift of the A leftward [p bit] is performed. The result is inputted into the cipher-processing section 551, the consecutive cipher-processing sections 552 and 553 which perform same processing, and the cipher-processing section which is not illustrated further, two or more step repeat operation is performed, and the enciphered block C is acquired from the data calcium and Cb outputted by the cipher-processing section 554 of the last stage.
[0035] Although the above explained drawing 2 and the data code circuit 115 of drawing 7 , in the data decoder circuit 116 of drawing 2 , the enciphered block can be decoded by calculating by the flow of the reverse of the code machine 1155. However, the operation 5516 of drawing 7 is considered as subtraction processing. Moreover, naturally the same key as the time of a code must be used for the sub keys KA and KB.
[0036] In addition, it may record on a tape as it is without enciphering packet data, when the permission is granted so that the program without the need of protecting

the packet data to record case [a program] for example, recorded may copy freely. This is realizable by switching the function passed without considering the data code circuit 115 and any data decoder circuits 116 as the function of the code and decode of an input packet. In drawing 2 and the data code circuit 115 of drawing 6 , with the processing-mode selection signal inputted through 1153d of processing-mode selection-signal input terminals of drawing 6 , although the input X5 to the operation 5516 of drawing 7 is not illustrated, a block can be passed by fixing to zero, without performing a code and decode processing. According to this approach, actuation can be switched, keeping the passage time delay of an input packet constant. Although not illustrated, as other approaches, moreover, the packet data inputted from the input terminal 1151 The block processing circuit 1152, the code machine 1155, and the block processing circuit 1156 are not minded. The switch circuit which switches whether it outputs to an output terminal 1157 or the packet data outputted from the block processing circuit 1156 are outputted to an output terminal 1157 is established in the preceding paragraph of an output terminal 1157. There is also the approach of switching the packet data which inputted into the switch circuit the processing-mode selection signal inputted through 1153d of processing-mode selection-signal input terminals, and were inputted into the packet data outputted from the block processing circuit 1156 and an input terminal 1157. These approaches are realizable with the same configuration as the above-mentioned also in drawing 2 and the data decoder circuit 116 of drawing 19 .

[0037] Drawing 8 is generation drawing of the data key in the data code circuit 115 of drawing 2 , and the control circuit 104 which shows the example of generation of the data key supplied to the data decoder circuit 116. The device key generator 117 has memorized the key information on the 96-bit immobilization defined beforehand. The block key generator 118 is a random number generator made to generate a 96-bit random number by the commander 1181 from the control circuit 104 of drawing 2 . 120 is a 96-bit EXCLUSIVE-OR-operation machine, and 121 is a Hash Function computing element. In drawing 8 (a), an exclusive OR is taken with the EXCLUSIVE-OR-operation vessel 120, with the Hash Function computing element 121, a hash operation is made and, as for a block key and a device key, 56 bits as which it was chosen of the result are supplied to the data code circuit 115 of drawing 2 as a data key. A Hash Function is a function with the output to input data difficult to guess, and the block key and device key which are confidential information are not called for from a data key.

[0038] Moreover, by generating the commander 1181 from the control circuit 104 of drawing 2 in a certain time interval, repeating the data key generation by the above-mentioned operation, and performing it, a sequential change of the data key can be made and it becomes possible to raise the safety of the data on a record medium. Next, the block key (Kr) generated by the block key generator 118 is sent to record digital-disposal-circuit 102a of drawing 2 , and is recorded on a tape 111.

[0039] Instead of the block key which the block key generator 118 generates at the time of playback, the same operation as the above is performed using the block key (Kp) reproduced from the tape 111, a data key is obtained, and the data decoder circuit 116 of drawing 2 is supplied.
[0040] Drawing 8 (b) is an example using what carried out EXCLUSIVE OR operation of the block key with the device key as key information Kr recorded on a tape 111. In this case, the block key itself is inputted into a Hash Function computing element. Instead of the block key in drawing 8 (a), at the time of playback, the same operation as the above is performed using Kp reproduced from the tape 111, a data key is obtained at it, and the data decoder circuit 116 is supplied.
[0041] Next, the record approach to a tape is described.
[0042] Drawing 9 is the record pattern of one truck. For the sub-code record section where 3 records sub-codes, such as a hour entry and program information, the data storage area where 7 records a digital compression video signal, and 2 and 6, as for the postamble of each record section, and 5, the gap between each record section, and 1 and 9 are [the preamble of each record section, and 4 and 8] the margins of a truck edge. Thus, each field can be independently postrecorded by preparing the postamble, the preamble, and the gap in each record section. Of course, digital signals other than a digital compression video signal may be recorded on a record section 7. The data storage area 7 is constituted by two or more blocks (it differs from the block which is the subunit of the above-mentioned encryption).
[0043] Drawing 10 is the block diagram of a block of the data storage area 7 of drawing 9 . For 20, as for ID information and 22, a synchronizing signal and 21 are [data and 23] the parity for the 1st error detection correction (C1 parity). For example, 3 bytes and data 22 consist of 99 bytes, parity 23 consists of 8 bytes, and 1 block of synchronizing signals 20 consists of 112 bytes for 2 bytes and the ID information 21.
[0044] Drawing 11 is the block diagram of the ID information 21 on drawing 10 . 31 is parity for a track address and 33 to detect the block address in 1 truck, and for 35 detect the error of the group number 31, a track address 32, and a block address 33, as for the group number and 32. A block address 33 is the address for identifying a block in each record section. For example, it is referred to as 0-335 in the data storage area 7 of drawing 9 . A track address 32 is the address for identifying a truck, for example, can change the address per one truck or 2 trucks, and can identify n truck. For example, six trucks are discriminable by being referred to as 0-5, or 0-2. The group number 31 of drawing 11 can identify 96 trucks by making it change per 6 trucks identified in a track address 32, and being referred to as 0-15. If a track address 32 is synchronized with the period of the 2nd error correcting code mentioned later, it can make easy processing at the time of record, and discernment at the time of playback.
[0045] Drawing 12 is the block diagram of the data for one truck of the data storage

area 7 of drawing 9 . In addition, the synchronizing signal 20 and the ID information 21 on the graphic display to drawing 10 are omitted. The data storage area 7 consists of 336 blocks, and data 41 are recorded on 306 blocks of the beginning, and it records the 2nd error correcting code (C2 parity) 43 on the following 30 blocks. C2 parity 43 is constituted per n truck unit, for example, 6 trucks. If it sees per 6 trucks, data are data of 306 block x6 truck, will divide the data into 18 and will add C2 10-block parity to each 102 block. A Reed Solomon code should just be used for an error correcting code. The data of 99 bytes of each block are constituted by 3 bytes of header 44, and 96 bytes of data 41.

[0046] Drawing 13 is the example of a configuration of a block of one packet when recording the digital compression video signal transmitted in 188 bytes of packet format on the data 41 of drawing 12 . In this case, 4 bytes of hour entry 25 is added, it considers as 192 bytes, and one packet is recorded on 2 blocks. A hour entry 25 is the information on time amount that the packet was transmitted. That is, data can be outputted in the same form as the time of being transmitted by counting time amount when the head of a packet is transmitted, or spacing between packets by the reference clock, recording the counted value with packet data, and setting up spacing between packets based on the information at the time of playback.

[0047] Drawing 14 is the block diagram of the header 44 of the data storage area 7 of drawing 12 . A header 44 is constituted by the format information 45, the block information 46, and additional information 47. In addition to this, auxiliary information is recorded for various recording information about record on the format information 45 and the block information 46 by additional information 47 again.

[0048] It is the information about a record format, and the copy limit information which shows whether the class of a recording mode (discernment of standard speed mode and others) and packet data to deal with and the packet data currently recorded can be copied is stored, and the format information 45 is two or more blocks, and constitutes one information. For example, one information consists of 12 blocks 12 bytes. And the ability to detect at the time of playback is raised by carrying out multiple-times repeat multiplex record of this information. It is possible to record the above-mentioned key information etc. here.

[0049] The block information 46 is the information for identifying the class of data recorded on a data storage area 41. Here, the existence of the data for high-speed adjustable-speed playback, a class (the data for high-speed adjustable-speed playback corresponding to which rate is it?), etc. are recorded. It is also possible to record the above-mentioned key information etc. here.

[0050] Additional information 47 can record the data of various classes, when the packed data which are one information are constituted from 6 blocks 6 bytes and 1 byte of the beginning uses the item code showing an informational class, and the remaining 5 bytes as data. For example, information, such as key information, such as the above-mentioned block key, and others, chart lasting time, the class of record

signal, etc. are recordable here.
[0051] Drawing 15 is the block diagram of the packed data in the case of storing a block key in the field of the additional information 47 of drawing 14 .
[0052] The item information code which shows that the information on consecutive is key information is stored in the first 1 byte of packed data.
[0053] The information (a key sequence number, a key attribute, key flag) which shows the class of key stored is recorded on the 2nd byte. As mentioned above, since the safety of the data on a record medium can be raised by making a sequential change of the block key with a certain time interval, the block key stored in this pack records the key attribute information which shows the block key used for the present packet data encryption, and the block key used for a degree, for example. Moreover, switch timing is recorded with the key flag reversed whenever a block key is updated. A switch of the key at the time of playback is made smooth using this information. Moreover, when a block key cannot be stored in one pack, the information which shows that there is a consecutive pack is stored in a key sequence number. For example, when a block key is 96 bits, it divides and stores in three packs, 2, 1, and 0 are stored in each key sequence number, and it is shown that 0 is the last pack. In addition, the size of the whole data is stored and there is also a method of getting to know the remaining magnitude.
[0054] To the 6th byte, a block key is contained from the 3rd byte.
[0055] In the example of above-mentioned drawing 8 (b), it is stored instead of the key information Kr being a block key.
[0056] Drawing 16 is drawing showing the storing approach of a block key. This example is the case where only the present key information is recorded on the packed data of each truck. Therefore, the above-mentioned key attribute is the constant of only the present key being shown, and it is not necessary to record it. (1) shows the condition that the 96-bit current block key A (A0 thru/or A11) is divided and stored in three packs, among this drawing. Usually, for improvement in the dependability of data, lessons is taken for these packs from one truck, and multiple-times record is carried out. For example, the effect of burst lack of a regenerative signal by the blinding of the magnetic head etc. is mitigable by what (a total of nine pieces) three packs are recorded on each last field for the beginning of a truck, and the middle. Moreover, it is not necessary to record three packs as a pack which not necessarily continued, and they insert the pack which stored other information between each pack, they are distributing and recording the pack which stores key information, the own protection of key information also becomes possible and its dependability improves further. This drawing (2) is packed data recorded on the truck with which the block key switched to B. In this case, the key flag of the block key B is reversed.
[0057] Drawing 17 is drawing showing other storing approaches of a block key. Drawing 17 is the approach of generating beforehand and also recording the key

information used for a degree with the present key information. Here, in the case of the block key which is used for "0" and a degree in the case of the block key used for a current packet data encryption, key attribute information is set to "1." Moreover, the key flag reversed whenever a block key is updated repeats "0" and "1" by turns.
[0058] (1) shows the condition that the 96-bit current block key A is stored, among this drawing. The following block key B is stored in (2). This (1) and (2) are recorded on the additional information area of the block in the same truck. (3) is packed data recorded on the truck with which the block key switched to B. In this case, the block key B has also reversed the key flag in the current lock of key attribute information "0" again. Furthermore, the key C which uses (4) for a degree is stored. (3) And (4) is recorded on a truck as packed data in the same truck.
[0059] There is also the approach of storing in the format information 45 shown in above-mentioned drawing 14 as a storing location of the key flag which shows the updating timing of a block key besides storing in the pack of additional information 47, or the block information 46.
[0060] As mentioned above, although key information is recorded on a tape, it is considering as the break eye of n truck (this example six trucks) which is the unit of addition of the C2 above-mentioned parity as timing which switches a block key, and at the time of playback, the operation of C2 parity is attained and the data reliability of key information improves.
[0061] Moreover, although the information which shows the timing by which a block key is updated was recorded as a key flag in the above example By synchronizing the value of the track address 32 shown in above-mentioned drawing 11 , or the group number 31, the period of the operation of C2 parity, and the timing of updating in record digital-disposal-circuit 102a of drawing 2 Even if it does not record especially a key flag, it is also possible to detect the timing of renewal of the key information at the time of playback with the value of this track address 32 or the group number 31. For example, in record digital-disposal-circuit 102a of drawing 2 , a track address 32 repeats the value of 0 to 5 for every one truck, and makes six trucks of the values 0-5 the unit of addition of the C2 above-mentioned parity. And a value updates and records a block key in the data code circuit 115 to the timing set to 0 from 5. What is necessary is to detect the timing to which the value of this track address 32 is set to 0 from 5, and just to update the key in the data decoder circuit 116 in regenerative-signal processing circuit 102b of drawing 2 , in the time of playback. Furthermore, in updating a long period, in case the value of a track address 32 is set to 0 from 5 using the group number 31, 1 **** of the group numbers 31 is carried out, and by making it repeat the value of 0 to 15, it is the unit of 96 trucks and it becomes possible to detect the timing of renewal of the break eye of the unit of addition of C2 parity moreover.
[0062] Drawing 18 is the example of a concrete configuration of the hour entry 25 (4 bytes = 32 bits) of drawing 13 , and shows a key flag and other approaches of code

flag storing. Here, it is the code flag (1 bit) which is 22-bit information as a hour entry 251, and shows whether, as for the key flag (1 bit) of the above-mentioned [252], and 253, consecutive packet data are enciphered, for example. At the time of record, the input/output control circuit 119 of drawing 2 stores "0", when consecutive packet data are enciphered by the code flag 253 with the hour entry 251 which is a time stump and "1" is not enciphered, and it stores in the key flag 252 at it the key flag of the packed data which store the above-mentioned key information corresponding to consecutive packet data. At the time of playback, in the input/output control circuit 119 of drawing 2 , while removing the hour entry 25 added at the time of record and outputting to the data decoder circuit 116, the code flag 253 and the key flag 252 are supplied to the data decoder circuit 116, and actuation of the data decoder circuit 116 is controlled.

[0063] Drawing 19 is the block diagram of the data decoder circuit 116 of drawing 2 . 1161 -- a packet data input terminal and 1167 -- a packet data output terminal, and 1163a and 1163b -- a data key input terminal and 1163c -- for a block processing circuit and 1164, as for a decoder, and 1168a and 1168b, a key schedule circuit and 1165 are [a processing-mode selection-signal input terminal, and 1162 and 1166 / a data key selection-signal input terminal and 1163d / a data key register and 1169] data key selectors. The data decoder circuit 116 is decrypted and outputted by the packet data unit inputted with the data key defined beforehand.

[0064] The block cipher which realizes decode processing by making into a unit the block which consists of two or more bits is used for a decoder 1165.

[0065] The packet data inputted from the input terminal 1161 are divided into the block C which consists of two or more bits like the data code circuit 115, and a sequential decryption is carried out in a decoder 1165, as a result, Block P is outputted, and in the block processing circuit 1166, each block is returned to the format of packet data, and outputs it to an output terminal 1167. Here, from a control circuit 104, the data key which is a key for a decryption is inputted from the data key input terminals 1163a and 1163b, and is memorized by the data key registers 1168a and 1168b. For example, the data key which switches the present data key to data key register 1168b at a degree is made to record on data key register 1168a.

[0066] Moreover, from 1163d of processing-mode selection-signal input terminals, the code flag 253 detected from the input/output control circuit 109 is inputted, and the mode of the decode actuation by the decoder 1165 and the mode passed without doing anything is determined. Furthermore, from data key selection-signal input terminal 1163c, the key flag 252 detected from the input/output control circuit 109 is inputted, and the data key chosen by the data key selector 1169 is outputted. The selected data key is changed into the sub keys KA and KB in the schedule circuit 1164, and is supplied to the code machine 1165.

[0067] Here, if the code flag detected in the input/output control circuit 119 of drawing 2 or a key flag changes, it will be interlocked with and selection of the mode

of operation of the data decoder 116 and a data key will be performed.
[0068] As mentioned above, the existence of encryption in a packet data unit, distinction of key information, and decode processing are realizable by adding a code flag and a key flag to each packet data.
[0069] In addition, there is also the approach of storing in the approach of storing in the 2nd byte of the pack which stores the key information shown in drawing 15 as a storing location of the code flag which shows whether it is enciphered or not or the format information 45 shown in above-mentioned drawing 14 , and the block information 46.
[0070] When packet data are enciphered by storing a code flag in the format information 45 or block information 46 grade when for example, a code flag shows "1" namely While considering actuation of the data decoder circuit 116 as decode actuation, acquire key information from the pack which stores the key information on additional information 47, and when a code flag is "0" Simplification of control action in case packet data are not enciphered can be attained by making it output actuation of the data decoder circuit 116 as it is without decoding. Moreover, by the approach of storing a code flag in the pack which stores key information, when "0", i.e., packet data, is not enciphered for the code flag, the block key information after the 3rd byte of the pack is not stored.
[0071] In addition, it can also distinguish whether it is enciphered by the existence of a pack which stores key information, without using a code flag.
[0072] Drawing 20 is the block diagram of the digital recording regenerative-signal processing circuit 102 which consists of record digital-disposal-circuit 102a of drawing 2 , and regenerative-signal processing circuit 102b. The memory control circuit which generates the address which 400 follows a memory circuit, and 401 follows the control circuit 104 of drawing 2 , and controls a memory circuit 400, In 402, C2 parity arithmetic circuit and 403 follow C1 parity arithmetic circuit, and 404 follows the content of setting out from said control circuit 104. ID information at the time of record, Addition of additional information, such as sub-code generation, format information, block information, and key information, And the additional information processing circuit which performs acquisition of additional information, such as ID information at the time of playback, a sub-code, format information, block information, and key information, etc., and 405 are strange demodulator circuits which perform modulation processing at the time of record, and recovery processing at the time of playback. In this example, since the data of six trucks are needed in order to perform C2 parity operation as an example, a memory circuit 400 shall be equipped with the capacity which stores the data for at least 6 trucks.
[0073] At the time of record, it is set as a record condition by the control circuit 104 of drawing 2 through terminals 411 and 413. The packet data enciphered in the data code circuit 115 of drawing 2 are inputted from a terminal 410, and are stored in a memory circuit 400 according to the control signal of the memory control circuit 401.

After data required for C2 parity operation are stored, it is serially read from a memory circuit 400, it is inputted into C2 parity arithmetic circuit 402, and a predetermined operation is performed. The result of an operation obtained in C2 parity arithmetic circuit 402 is accumulated in a memory circuit 400. On the other hand, through a terminal 413, according to setting out from the control circuit 104 of drawing 2 , packed data, such as key information corresponding to the key of the inputted encryption packet data, are generated, and it is accumulated in a memory circuit 400 in the additional information processing circuit 404. it is reading from a memory circuit 400 including key information etc. so that said record block carried out may furthermore be constituted -- C1 parity is added to the data carried out in C1 parity arithmetic circuit 403, and they are inputted into the strange demodulator circuit 405. The signal by which modulation processing of predetermined was carried out by the strange demodulator circuit 405 is outputted through a terminal 414, and is recorded on a tape 111 through the record playback amplifier 116 of drawing 2 , and a rotary head 100.

[0074] Drawing 21 is drawing showing the timing of signal processing at the time of data-logging initiation. The packet data inputted from the data encryption circuit 115 and drawing 21 (b) drawing 21 (a) The data key used when the data encryption circuit 115 was encryption, and drawing 21 (c) In accordance with 6 truck unit configurations of the C2 above-mentioned parity 43, C2 parity operation cycle (this example six trucks) in C2 parity arithmetic circuit 402 of drawing 20 is shown, and drawing 21 (d) shows the record signal recorded on a tape 111 through a rotary head 100. In the example of drawing 21 , the block key A is beforehand generated before the time amount t1 to which a recording start is set, the data key Ka is calculated, and the data encryption circuit 115 is supplied. Moreover, record digital-disposal-circuit 102a controls a front [time amount / t1 / to which a recording start is set] to consider that he has no ****** packet to an input signal, and to perform record signal processing. Thereby, even if a recording start is set as time amount t0, the operation of C2 parity to the data of a period p0 becomes possible.

[0075] C2 parity operation cycle s0 of the input data when making it a recording start by time amount t0 is completed, and the control circuit 104 of drawing 2 outputs and (drawing 21 (d)) controls a record signal from the head which is n truck (this example six trucks) which constitutes said 2nd error correcting code. Moreover, a data key is updated in the operation cycle of this C2 parity. For example, the block key B is generated before time amount t2, the data key Kb is calculated, the data encryption circuit 115 is supplied, and a data key is switched to Kb in the data encryption circuit 115 at the event of time amount t2. Usually, a time delay produces the data encryption circuit 115 from a packet entry of data before an output for the processing. Then, the data key supplied to the data encryption circuit 115 is switched to Kb at the event of the data time delay quota produced when the data encryption circuit 115 carries out encryption processing of the packet from time amount t2. Or

from the packet data with which the data key was switched, you may postpone to processing of the following operation cycle. Although excessive data are recorded on a head part in this example, it is not based on the timing of the time amount t1 made into a recording start, but C2 parity is added to the signal which should be recorded, and it can record per [above-mentioned] C2 parity operation cycle. Moreover, since it considers that a part for data division with an excessive head has no packet and record processing is carried out at the time of playback, it is only used for C2 parity operation, and is not outputted.

[0076] At the time of record termination, it controls by said control circuit 104 to perform record actuation to the tape 111 of said record regenerative-signal processing circuit 102a by the operation cycle (this example six trucks) conclusion of C2 parity calculated using the data of a multiple track. Since it is not based on the change timing of a recording start and record termination, but C2 parity is altogether added to the record data on a tape 111 with this control system, key information is updated per operation cycle of C2 parity and packet data are enciphered, at the time of playback, it is reproducible per C2 parity operation cycle, and since C2 parity operation is attained, the data reliability of key information also improves.

[0077] Drawing 22 is drawing showing the key information on the tape 111 of drawing 2 . 1111-1117 are the recording tracks shown per 6 trucks which are C2 parity operation cycle among this drawing. In the case of this drawing, the packed data even whose recording tracks 1111-1113 even the block key A and recording tracks 1114-1116 are the packet data with which it was enciphered based on the block key B, and the key information corresponding to them are stored. Moreover, a recording track 1117 is a truck recorded without being enciphered. The enciphered truck and the truck which is not enciphered are able to be intermingled on the same tape, as shown in this drawing. Although every mxn trucks (m is one or more integers and n is 6 at this example), such as 48 trucks and 96 trucks, the one whole program, etc. are considered, as for the renewal of key information, a key switches, and the boundary line of an eye or the enciphered truck, and the truck which is not enciphered is a break eye of C2 parity operation cycle (this example six trucks).

[0078] In the above, the actuation in the case of record was explained. Here, although it is also possible to record key information on a sub-code field (7 of drawing 9), key information is stored in the part of the header (44 of drawing 12) of each block, and rewriting of only the key information by postrecording etc. becomes difficult by recording on the data storage area on each truck (7 of drawing 9). Therefore, it is effective in the ability to prevent disappearance of key information, and not alter only key information intentionally, and not perform cryptocommunication intentionally.

[0079] Next, the playback approach from a tape is described.

[0080] In the digital recording regenerative-signal processing circuit 102 of drawing 20 , it is set as a playback condition by the control circuit 104 of drawing 2 through terminals 411 and 413 at the time of playback. After recovery processing of the

regenerative signal which was reproduced by the rotary head 100 from said tape 111, and was inputted from the terminal 414 is carried out in the strange demodulator circuit 405, C1 parity operation is performed in C1 parity arithmetic circuit 403, error detection and its correction are performed, and C1 parity result of an operation is also accumulated in a memory circuit 400 together. After data required for C2 parity operation are stored, according to the control signal of the memory control circuit 401, it is serially read from a memory circuit 400, and is inputted into C2 parity arithmetic circuit 402. In C2 parity arithmetic circuit 402, it calculates by the above-mentioned data and detection of an error, the data which carried out correction processing, and C2 parity result of an operation are again accumulated in a memory circuit 400.

[0081] Data are read from a memory circuit 400 in predetermined sequence on the basis of the timing signal inputted through a terminal 412 from the timing generation circuit 105 of drawing 2 , and only data without an error are outputted to the input/output control circuit 119 of drawing 2 from a terminal 410 with reference to the result of an operation of said C1 parity and C2 parity. On the other hand, in the additional information processing circuit 404, key information, a sub-code, etc. are acquired from the data read from the memory circuit 400, and it sends out to the control circuit 104 of drawing 2 through a terminal 413. Then, an exclusive OR with the device key from ejection and the device key generator 117 is taken for Kp, Hash Function 121 is calculated, a data key is obtained from the operation shown by drawing 8 , i.e., the key information acquired by playback, and it outputs to the data decoder circuit 116 of drawing 2 . This data key is the same as the data key used at the time of record, and the packet data of a basis can be correctly obtained in the data decoder circuit 116.

[0082] Drawing 23 is drawing showing the timing of signal processing at the time of data playback of this invention. Drawing 23 (a) shows the packet data with which the regenerative signal and drawing 23 (b) which are reproduced from a tape 111 through a rotary head 100 show the operation cycle (this example six trucks) of the C2 above-mentioned parity, and drawing 23 (c) is outputted from the input/output control circuit 119, and drawing 23 (d) shows the data key supplied to the data decoder circuit 116 of drawing 2 . In the additional information processing circuit 404, the key information KpC used in this cycle is detected in the operation cycle s3. The data key Kc obtained by this KpC by the above-mentioned operation is memorized by the above-mentioned data key register 1163a, and the data key selector 1169 is also chosen so that the data key Kc of data key register 1163a may be outputted.

[0083] Next, in the operation cycle s4, if it is detected that the key information KpD is used, it will ask for the data key Kd by the above-mentioned operation, will make data key register 1163b memorize beforehand, will control the data key selector 1169 by timing of time amount t3, and will switch to the data key Kd of data key register 1163b. By the above approach, playback actuation while updating a data key is

attained.
[0084] Moreover, bond record is attained, without spoiling the data reliability of the key information on the truck in front of additional record by starting record from the break eye of the addition unit of C2 parity on a tape [finishing / record / already], when carrying out additional record.
[0085] in addition, as an approach of distinguishing, whether there is any paddle with which packet data are enciphered Since the synchronous cutting tools 501 who showed by drawing 4 are usually fixed data, in regenerative-signal processing circuit 102b, detect this synchronous cutting tool, and when it is able to detect, for example When it is not able to switch and detect to the function passed without carrying out any packet data into which the data decoder circuit 116 of drawing 2 is inputted By performing actuation which detects the key information in a switch and additional information area for the data decoder circuit 116 of drawing 2 in actuation of a decode function It becomes detectable also when it is the tape on which the truck which enciphered packet data and was recorded at the time of record, and the truck recorded without enciphering are intermingled.
[0086] Moreover, also with the software tape currently recorded beforehand, by the approach which explained above, it becomes creation of a software tape, and reproducible, and protection of the packet data on a tape can be realized.
[0087] Although the above showed the example in which the present block key is stored in the recording track, the operation of a data key must be performed within the 1 operation cycle of C2. When the operation of a data key does not meet the deadline within the 1 operation cycle of C2, as mentioned above, it is recording the present block key and the following block key in a recording track, and can set in quest of the following data key beforehand.
[0088] Drawing 24 is other block diagrams of the digital signal record regenerative apparatus 200 of drawing 1 . 121 are a digital interface circuitry which realizes protocols, such as a high-speed digital bus interface like IEEE1394, among this drawing, and 122 which has the function to transmit data to a high speed is a digital interface bus, maintaining the time interval of the inputted packet data. 123 is the code/decoder circuit for protecting the digital data transmitted in the digital interface 122 top, and decrypts the digital data which enciphered packet data, and transmitted on the digital interface bus 122, or was received. 124 is a control circuit like a microprocessor and controls the digital interface circuitry 121, and the code/decoder circuit 123.
[0089] At the time of record, in the digital interface circuitry 121, predetermined packet processing is performed, and the enciphered digital data which has been transmitted in the digital interface bus 122 top is decoded to the original packet data in a code / decoder circuit 123, and is outputted to the I/O circuit 107. Then, as the above-mentioned explained, packet data are enciphered in the data code circuit 115, and it records on a tape 111. At the time of playback, the reproduced packet data are

decrypted in the data decoder circuit 116, and from the I/O circuit 107, it outputs to a code / decoder circuit 123, it enciphers in a code / decoder circuit 123, and outputs to the digital interface bus 122 from the digital interface circuitry 121. According to this, protection of the both sides of the packet data on a tape and the packet data on a digital interface bus is realizable.

[0090] Next, the example in an optical disk is explained.

[0091] Drawing 25 is the block diagram of the file currently recorded on the disk. 601 is a lead-in groove field and various parameters are stored. 602, 603, and -- are program 1 field, program 2 field, and --, and a program different, respectively etc. is stored in each program field.

[0092] Drawing 26 is the block diagram of one program field, for example, program 1 field. A program field consists of two or more units, and carries out piece storing of the sequence which is one unit of the digital compression video signal later mentioned to each of this unit, for example.

[0093] the intra into which drawing 27 was compressed per frame of a digital compression video signal -- prediction [data / frame data and / of the frame of order] -- using -- difference -- it is the relation of the INTAFUREMU data which compressed only information. 621 -- intra -- a frame and 622 are INTAFUREMU. a digital compression video signal -- the frame of a predetermined number, for example, 15 frames, -- one sequence -- carrying out -- the head -- intra -- a frame 621 -- carrying out -- the remaining frames -- intra -- it is considering as INTAFUREMU 622 compressed using the prediction from a frame 621. of course, except for a head -- intra -- you may make it arrange a frame 621

[0094] Drawing 28 is the configuration of a digital compression video signal. The picture header to which 623 is added per frame, and 624 are sequence headers added per sequence. The sequence header 624 is constituted by information, such as a synchronizing signal and a transmission rate. the picture header 623 -- a synchronizing signal and intra -- it is constituted by the identification information of a frame or INTAFUREMU etc. Usually, the die length of each data changes with amount of information. One sequence is stored in the one above-mentioned unit.

[0095] Each unit of above-mentioned drawing 26 is constituted by two or more data sectors.

[0096] Drawing 29 is the block diagram of each data sector. 631 -- ID information -- 4 bytes and 632 -- the parity for error detection correction of the ID information 631 -- 2 bytes and 633 -- with management data, 6 bytes and 634 consist of user data, and 2048 bytes and 635 are constituted from 4 bytes by the parity for error detection correction of the user data 634. Among these, the digital compression video signal shown by drawing 28 is divided and stored in user data 634. In addition, a digital compression speech compression signal is also divided and is stored in user data 634. The one above-mentioned unit is the meeting of the data sector in which the digital compression video signal and the sound signal were stored, respectively.

[0097] Drawing 30 is the block diagram which added the error correcting code added in case a data sector is recorded on a disk. First, a data sector is divided into 172 bytes and 10 bytes of parity [a part of] 637 for the 1st error detection correction (a part of C1 parity parity 637) is added to it. Furthermore these n data sectors (for example, this example 16 pieces) are collected, and 16 parity 636 (C2 parity 636) for the 2nd error detection correction is shortly added to 192 bytes of a line writing direction. 10 bytes of C1 parity [a part of] 637 is added also to C2 obtained parity 636.

[0098] Drawing 31 is the block diagram of the digital signal record regenerative apparatus which used the optical disk as a record medium. The record digital disposal circuit to which 701 perform an optical disk among this drawing, and, as for an optical pickup and 703a, 702 performs generation of the record signal at the time of record etc., The regenerative-signal processing circuit where 703b performs the recovery of the regenerative signal at the time of playback etc., a control circuit [like a microprocessor] whose 704 is, A spindle motor and 706 705 The rotational speed of an optical disk 701, and the location of an optical pickup 702, The servo circuit which controls a focus, the data code circuit at the time of digital signal record of the term configuration as drawing 6 with 709 [same], The data decoder circuit at the time of digital signal playback of the configuration as drawing 19 with 710 [same] and 711 The device key generator which generates the device key which is the basis of the data key which supplies a digital signal to the data code circuit 709 or the data decoder circuit 710 a code or in case it decodes, The disk key generator which generates the disk key whose 712 is another basis of a code or the data key at the time of decoding about digital information, As for the block key generator by which 713 generates the block key a code or whose data key at the time of decoding is another basis further about digital information, and 719, a digital interface circuitry and 720 are input/output terminals.

[0099] At the time of record, digital signals, such as a digital compression video signal divided into the format of the user data 634 of the data sector of drawing 29 , are inputted into the digital interface circuitry 719 from an input/output terminal 720. In the data code circuit 709, with the data key generated in a control circuit 704 based on the key generated by the device key generator 711, the disk key generator 712, and the block key generator 713, the inputted digital signal enciphers the inputted digital signal, and outputs this to record digital-disposal-circuit 703a. In record digital-disposal-circuit 703a, ID631 of drawing 29 , parity 632, management data 633, and parity 635 are added to the inputted digital signal of user data format, and it is made the format of a data sector. Next, although C1 parity 637 of drawing 30 and C2 parity 636 are added by making n data sectors into a unit (this example 16 pieces) and not being illustrated further, predetermined rearrangement and a header are added, modulation processing is performed, and it is recorded on an optical disk 701 through an optical pickup 702.

[0100] Drawing 32 is the example of generation of the data key supplied to the data code circuit 709, for example, these generation is performed in the control circuit 704 of drawing 31 . The device key generator 711 has memorized the key information on the 96-bit immobilization defined beforehand. The disk key generator 712 and the block key generator 713 are random number generators made to generate a 96-bit random number by the commanders 7121 and 7131 from the control circuit 704 of drawing 31 . As for 721 and 722, a 96-bit EXCLUSIVE-OR-operation machine and 723 are Hash Function computing elements. First, a hash operation is made with the Hash Function computing element 723, and, as for a block key, 56 bits of the result are supplied to the data code circuit 709 of drawing 31 as a data key. Moreover, an exclusive OR is taken with a 96-bit disk key and the EXCLUSIVE-OR-operation vessel 722 (henceforth the key information Kr), and a 96-bit block key is sent to record digital-disposal-circuit 703a of drawing 31 , and is recorded on an optical disk 701. Furthermore, an exclusive OR is taken with the EXCLUSIVE-OR-operation vessel 721 (henceforth the key information kd), and a disk key and a device key are sent to record digital-disposal-circuit 703a of drawing 31 , and are recorded on an optical disk 701 through an optical pickup 702.

[0101] Here, by generating the commander 7131 from the control circuit 704 of drawing 31 in a certain time interval, repeating generation of the data key by the above-mentioned operation, and performing it, a sequential change of the data key can be made and it becomes possible to raise the safety of the data on an optical disk. Moreover, a commander 7121 makes it generate once in the case of one record actuation. Or in case it records on an empty optical disk first, it is made to generate only once and kd is recorded, from the next record actuation, the above-mentioned key information kd on an optical disk is once reproduced, and there is also a method of taking a block key and an exclusive OR using the disk key obtained by taking a device key and an exclusive OR, and acquiring the key information kr. Furthermore, the key information kd is beforehand recorded in the manufacture process of an optical disk, the kd is reproduced before record actuation, without using the disk key generator 712, and there is also a method of obtaining a disk key. The key information kd is recorded on the lead-in groove field 601 of drawing 25 .

[0102] The key information kd is reproduced first, in the case of playback, a disk key is obtained by taking an exclusive OR for the key information kd and a device key, an exclusive OR is taken for the key information kr reproduced further and the obtained disk key at it, a block key is obtained, and the data key inputted into the data decoder circuit 710 of drawing 31 is obtained by calculating Hash Function 723.

[0103] In drawing 31 , while the regenerative signal reproduced from the optical pickup 702 is inputted into regenerative-signal processing circuit 703b and performing recovery and error detection correction in regenerative-signal processing circuit 703b in the case of playback, the digital signal of the format of the user data 634 of drawing 29 is outputted to the data decoder circuit 710. In regenerative-signal processing

circuit 703b, playback of a disk key and block key information is also performed, and it sends to a control circuit 704. In a control circuit 704, the above-mentioned data key playback is calculated and the data decoder circuit 710 is supplied. In the data decoder circuit 710, the digital signal from regenerative-signal processing circuit 703b is decoded, and it is outputted from an input/output terminal 720 through the digital interface circuitry 719.

[0104] In addition, when the digital signal to record does not need to be protected, you may record on an optical disk as it is without enciphering.

[0105] Drawing 33 is the block diagram of the management data 633 of drawing 29 . The above-mentioned key information kr is stored in this management data 633. The key sequence number which shows that the code flag which shows whether the user data whose 6341 is the data sector in which this management data 633 is stored are enciphered, the data effective flag with which the key information for which 6342 is stored in this management data shows validity or an invalid, and 6343 have consecutive management data when the key information kr cannot store in one management data 633, and 6344 are the key information kr.

[0106] Drawing 34 is drawing showing how to store the key information kr in the field of the management data 633 of drawing 29 . In this example, the 64-bit above-mentioned key information is stored for the management data of 16 data sectors (the data sector 0 - data sector 015) which are the addition units of C2 parity 636 of drawing 30 as one unit. The 96-bit key information kr is divided and stored in three management data kr0, kr1, and kr2. In that case, "1" 1" which shows that the code flag 6341 is enciphered indicates it to be that a data effective flag is effective stores 2, 1, and 0 in three management data in order again, and the key sequence number 6343 shows that it is the last of division of 0. These are repeatedly stored in 16 management data. However, since the last management data becomes odd, "0" which shows that a data effective flag is invalid is stored.

[0107] As mentioned above, key information is recorded on an optical disk. At this time, key information is updated considering 16 pieces or the data sector of that integral multiple as a unit. Although it is possible to perform renewal of this key information for every (for m to be one or more integers and for n to be 16 at this example) mxn data sectors, such as 64 data sector and a 128 data sector, a key switches and an eye or the boundary line of the existence of encryption is a break eye of the addition unit (this example 16 data sector) of C2 parity. By this, the operation of C2 parity is attained at the time of playback, and the data reliability of key information improves.

[0108] In addition, record digital-disposal-circuit 703a and regenerative-signal processing circuit 703b perform actuation of the digital recording regenerative-signal processing circuit 102 of drawing 20 , and same actuation. However, the addition unit of C2 parity turns into n data sector unit (this example 16 data sector).

[0109] Drawing 35 is other block diagrams of the digital signal record regenerative

apparatus which used the optical disk as a record medium. In this example, it is an example in the case of carrying out record playback of the fixed-length packet of the digital image compression signal shown in drawing 3 at an optical disk 701. Among drawing 35 , 717 are a digital interface circuitry which realizes protocols, such as a high-speed digital bus interface like IEEE1394, and they have the function to transmit data to a high speed, maintaining the time interval of the inputted packet data. 718 is a digital interface bus. 715 is the code/decoder circuit for protecting the digital data transmitted in the digital interface 718 top, and decrypts the digital data which enciphered packet data, and transmitted on the digital interface bus 718, or was received. 716 is a control circuit like a microprocessor and controls the digital interface circuitry 717, and the code/decoder circuit 715. The sector conversion circuit to which 707 picks out packet data from conversion or user data for packet data to the user data of a data sector, and 708 are input/output control circuits which perform the output control of the time stump processing to the packet data at the time of record, and the packet data at the time of playback.

[0110] At the time of record, predetermined packet processing is performed to the enciphered digital data which has been transmitted in the digital interface bus 718 top in the digital interface circuitry 717, and it decodes to the original packet data in a code / decoder circuit 715, and outputs to the I/O circuit 714. Then, packet data are enciphered in the data code circuit 709, and a time stump is given to the packet data inputted in the input/output control circuit 708, and it outputs to the sector conversion circuit 707. The inputted packet data are changed into the format of the user data of the above-mentioned data sector in the sector conversion circuit 707. The digital signal changed into the format of user data is recorded on an optical disk 701 through record digital-disposal-circuit 703a and an optical pickup 702.

[0111] Therefore, said key information is recorded on the predetermined field with said digital signal enciphered with the key obtained by carrying out a predetermined operation to key information on the optical disk 701. Moreover, said digital signal comes to have the packet format of predetermined length. Furthermore, said key information is updated at intervals of predetermined, and is recorded on the predetermined field. Furthermore, the conversion digital signal changed with two or more kinds of keys and said key are recorded.

[0112] At the time of playback, the packet data with which output timing was controlled through an optical pickup 702 and record digital-disposal-circuit 703a based on the time stump to which packet data were added in ejection and the input/output control circuit 708 in the sector conversion circuit 707 at the time of record from the reproduced user data, and the time stump was removed are outputted. Furthermore, in the data decoder circuit 710, the reproduced packet data are decrypted, and from the I/O circuit 714, it outputs to a code / decoder circuit 715, it enciphers in a code / decoder circuit 715, and outputs to the digital interface bus 718 from the digital interface circuitry 717.

[0113] Drawing 36 is the block diagram of the packet data stored in the user data 634 of the data sector of drawing 29 changed by the sector conversion circuit 707 of drawing 35 . Two or more fixed-length packets of a digital image compression signal are stored. In the input/output control circuit 708 of drawing 35 , 4 bytes of hour entry 642,644 and -- are added to each packet 643,645 and --. When a data sector is 2048 bytes, ten packets to which the hour entry was added can be stored. The packet to which the hour entry was added does not need to be stored continuously, and may have a free space on the way. Moreover, the break eye of a packet can be easily distinguished by adding a packet header 641.
[0114] Also in this example, it is considering as the break eye of n data sector (this example 16 data sector) which is the addition unit of this C2 parity as a boundary line of the timing which switches the above-mentioned key information, or the existence of encryption, and the operation of C2 parity is attained at the time of playback, and the data reliability of key information improves.
[0115] Drawing 37 is each hour entry 642,644 of drawing 36 , and the block diagram of --. The code flag 651 is a flag which shows whether the packet is enciphered or not, and a key flag is a flag which shows with which key it is enciphered, when this packet is enciphered. For example, the value which increases every [1] with 0, 1, 2, and 3 whenever a key is updated can be taken being able to use this flag as 2 bits, and the key which corresponds for every packet can be specified by storing the same flag also in the management data of drawing 29 . These flags may be stored in the above-mentioned packet header 641. According to this approach, it becomes possible for every packet to update a key to arbitration.
[0116] In addition, in the above example, although record playback with a magnetic tape and an optical disk was explained, even when carrying out record playback, it can apply to a magnetic disk and all other record media, such as semiconductor memory, similarly.
[0117] In the case of the above-mentioned semiconductor memory, a switch of whether key information switches or enciphers or not to carry out is good to carry out by the break eye of the address which is one unit of record of semiconductor memory.
[0118] Moreover, this example applies this invention to the system which enciphers a digital signal with a key. However, this invention is not limited to this example and can be applied also to the system by which a digital signal is scrambled by the keycode. That is, this invention is applicable to all the systems processed so that it may be changed from the clear condition that a digital signal is from the first, at least.
[0119]
[Effect of the Invention] In the digital signal recording device which records or reproduces a digital signal on a record medium according to this invention, a regenerative apparatus, and a record medium at the time of record With the key obtained by performing a predetermined operation to key information, a digital signal is

enciphered, with said key information, it records on a record medium, and the reproduced digital signal is decrypted and outputted to said key information reproduced from the record medium with the key obtained by performing said predetermined operation at the time of playback. By the above, even if it acquires the key information on a record medium since said key is not obtained unless said predetermined operation is performed, in the case of playback, it is difficult to decode the digital signal enciphered using it, and the copyright of the digital signal on a record medium can be protected at it.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram which contains a digital broadcast receiver and a digital signal record regenerative apparatus in the example of this invention.
[Drawing 2] It is the block diagram of the digital signal record regenerative apparatus 200 of drawing 1 .
[Drawing 3] It is the block diagram of the packet of a digital image compression signal.
[Drawing 4] It is the block diagram of the packet header 306 of drawing 3 .
[Drawing 5] It is the block diagram of the signal chosen from the transmission signal and transmission signal of digital broadcast.
[Drawing 6] It is the block diagram of the data code circuit 115 of drawing 2 .
[Drawing 7] It is the block diagram of the code machine 1155 of drawing 6 .
[Drawing 8] It is generation drawing of the data key in the data code circuit 115 of drawing 2 , and the control circuit 104 which shows the example of generation of the data key supplied to the data decoder circuit 116.
[Drawing 9] It is drawing showing the record pattern of one truck of a tape 111.
[Drawing 10] It is the block diagram of a block of the data storage area 7 of drawing 9 .
[Drawing 11] It is the block diagram of the ID information 21 on drawing 10 .
[Drawing 12] It is the block diagram of the data for one truck of the data storage area 7 of drawing 9 .
[Drawing 13] It is the block diagram of a block of one packet when recording the digital compression video signal transmitted in 188 bytes of packet format on the data 41 of drawing 12 .
[Drawing 14] It is the block diagram of the header 44 of the data storage area 7 of drawing 12 .
[Drawing 15] It is the block diagram of the packed data in the case of storing a block key in the field of the additional information 47 of drawing 14 .

[Drawing 16] It is drawing showing the storing approach of a block key.
[Drawing 17] It is drawing showing other storing approaches of a block key.
[Drawing 18] It is the concrete block diagram of the hour entry 25 of drawing 13 .
[Drawing 19] It is the block diagram of the data decoder circuit 116 of drawing 2 .
[Drawing 20] It is the block diagram of the digital recording regenerative-signal processing circuit 102 which consists of record digital-disposal-circuit 102a of drawing 2 , and regenerative-signal processing circuit 102b.
[Drawing 21] It is drawing showing the timing of signal processing at the time of data-logging initiation.
[Drawing 22] It is drawing showing the key information on the tape 111 of drawing 2 .
[Drawing 23] It is drawing showing the timing of signal processing at the time of data playback.
[Drawing 24] They are other block diagrams of the digital signal record regenerative apparatus 200 of drawing 1 .
[Drawing 25] It is the block diagram of the file currently recorded on the disk.
[Drawing 26] It is the block diagram of one program field.
[Drawing 27] the intra of a digital compression video signal -- it is drawing showing the relation between frame data and INTAFUREMU data.
[Drawing 28] It is the block diagram of a digital compression video signal.
[Drawing 29] It is the block diagram of a data sector.
[Drawing 30] It is the block diagram which added the error correcting code added in case a data sector is recorded on a disk.
[Drawing 31] It is the block diagram of the digital signal record regenerative apparatus using the optical disk as a record medium.
[Drawing 32] It is drawing showing the example of generation of the data key supplied to the data code circuit 709.
[Drawing 33] It is the block diagram of the management data 633 of drawing 29 .
[Drawing 34] It is drawing showing how to store the key information kr in a management data field.
[Drawing 35] They are other block diagrams of the digital signal record regenerative apparatus using the optical disk as a record medium.
[Drawing 36] It is the block diagram of the packet data stored in the user data 634 of the data sector of drawing 29 .
[Drawing 37] It is the block diagram of the hour entry in the case of adding a code flag etc. to the above-mentioned hour entry.
[Description of Notations]
7 [-- Data,] -- A data storage area, 20 -- A synchronizing signal, 21 -- ID information, 22 25 [-- Block address,] -- A hour entry, 31 -- The group number, 32 -- A track address, 33 41 [-- Block information,] -- Video-signal data, 44 -- A header, 45 -- Format information, 46 47 [-- Capstan,] -- Additional information, 71 -- A packet, 100 -- A rotary head, 101 102a -- A record digital disposal circuit, 102b

-- A regenerative-signal processing circuit, 104 -- Control circuit, 105 -- A timing generation circuit, 106 -- A servo circuit, 107 -- I/O circuit, 109 -- A timing-control circuit, 110 -- An oscillator circuit, 115 -- Data code circuit, 116 -- A data decoder circuit, 117 -- A device key generator, 118 -- Block key generator, 119 -- An input/output control circuit, 200 -- A digital signal record regenerative apparatus, 201 -- Digital broadcast receiver, 203 [-- Interface circuitry,] -- A tuner, 204 -- A selection circuitry, 205 -- A decoder circuit, 206 208 -- A control circuit, 1152 -- A block processing circuit, 1154 -- Key schedule circuit, 1155 -- A code machine, 1158 -- A data key register, 1159 -- Data key selector, 1165 [-- C2 parity arithmetic circuit 403 / -- C1 parity arithmetic circuit, 404 / -- An additional information processing circuit, 405 / -- A strange demodulator circuit, 551 / -- Cipher-processing section.] -- A decoder, 400 -- A memory circuit, 401 -- A memory control circuit, 402 701 [-- A regenerative-signal processing circuit 704 / -- A control circuit, 705 / -- A spindle motor, 706 / -- A servo circuit, 707 / -- A sector conversion circuit, 708 / -- An input/output control circuit, 709 / -- A data code circuit, 710 / -- A data decoder circuit, 711 / -- A device key generator, 712 / -- A disk key generator, 713 / -- A block key generator, 719 / -- Digital interface circuitry.] -- An optical disk, 702 -- An optical pickup, 703a -- A record digital disposal circuit, 703b

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－293936
（P2000－293936A）
(43)公開日　平成12年10月20日(2000.10.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０５３
	３０１		３０１Ｚ	５Ｄ０４４
20/12	１０２	20/12	１０２	
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	
5/92		5/92	Ｈ	

審査請求　未請求　請求項の数28　ＯＬ　（全 28 頁）

(21)出願番号　特願平11－100976

(22)出願日　平成11年４月８日(1999.4.8)

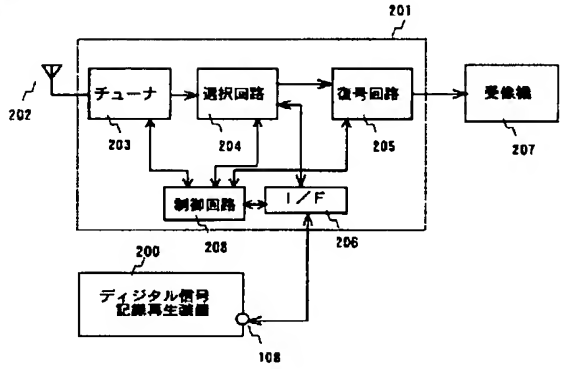
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　佐々本　学
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　岡本　宏夫
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ディジタル信号記録装置、再生装置、および記録媒体

(57)【要約】
【課題】記録媒体上のディジタル信号の著作権を保護できる記録装置、再生装置、および記録媒体を提供することにある。
【解決手段】ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力することにより達成できる。

図１



【特許請求の範囲】
【請求項１】ディジタル信号を記録媒体上に記録するディジタル信号記録装置において、
少なくとも一つの鍵情報を発生する鍵情報発生手段と、
前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、
前記鍵と前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を暗号化して出力する暗号変換手段と、
少なくとも一つの前記鍵情報を、暗号化された前記ディジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを備えたことを特徴とするディジタル信号記録装置。
【請求項２】前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項１記載のディジタル信号記録装置。
【請求項３】前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を備え、
前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記記録媒体上の所定の領域に記録する機能を備えたことを特徴とする請求項１記載のディジタル信号記録装置。
【請求項４】前記ディジタル信号は、所定長のパケット形式を有してなり、
前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記ディジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求項３記載のディジタル信号記録装置。
【請求項５】前記暗号変換手段は、さらに、前記ディジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を備え、
前記記録手段は、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、暗号化しない場合は、前記鍵情報を記録しない機能を備えたことを特徴とする請求項１記載のディジタル信号記録装置。
【請求項６】前記ディジタル信号は、所定長のパケット形式を有してなり、
前記記録手段は、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、前記ディジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求項５記載のディジタル信号記録装置。
【請求項７】所定長のディジタル信号を入力して、同期信号、管理情報信号を付加してセクタ形式とし、前記セクタに第１の誤り訂正符号を付加し、さらにｎ（ｎは１以上の整数）セクタ単位で第２の誤り訂正符号を付加し、前記第２の誤り訂正符号にも第１の誤り訂正符号を付加して記録媒体上に記録するディジタル信号記録装置において、
少なくとも一つの鍵情報を発生する鍵情報発生手段と、
前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、
前記鍵と前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を暗号化して出力する暗号変換手段と、
少なくとも一つの前記鍵情報を、暗号化された前記ディジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを備えたことを特徴とするディジタル信号記録装置。
【請求項８】前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を有し、
前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、前記所定の演算を行って更新された鍵を発生し、
前記暗号変換手段は、前記第２の誤り訂正符号を付加したｎセクタの単位の区切り目で、前記更新された鍵に切り換える機能を備えたことを特徴とする請求項７記載のディジタル信号記録装置。
【請求項９】前記暗号変換手段は、前記ディジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を有し、
前記記録手段は、前記ディジタル信号が暗号化されているか否かを示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、
前記第２の誤り訂正符号を付加したセクタの単位の区切り目で、前記ディジタル信号を暗号化するか否かを切り換える機能を備えたことを特徴とする請求項７記載のディジタル信号記録装置。
【請求項１０】記録媒体上に記録されているディジタル信号を再生するディジタル信号再生装置において、
前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記ディジタル信号とを再生する再生手段と、
前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、
前記鍵と再生された前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を復号化して出力する復号変換手段とを備えたことを特徴とするディジタル信号再生装置。
【請求項１１】前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項１０記載のディジタル信号再生装置。
【請求項１２】少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、
前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力されて所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求項１０記載のディジタル信号再生装置。
【請求項１３】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情

報と、前記鍵情報を更新するタイミングを識別可能な情報とを、再生する機能を備え、
前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、
前記復号変換手段は、入力された前記鍵を、前記タイミング信号に合わせて前記更新された鍵に切り換える手段を備えたことを特徴とする請求項１０記載のディジタル信号再生装置。
【請求項１４】前記ディジタル信号は、所定長のパケット形式を有してなり、
前記再生手段は、前記ディジタル信号の各パケットに付加して記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求項１３記載のディジタル信号再生装置。
【請求項１５】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備え、
前記復号変換手段は、前記暗号フラグ情報により、再生された前記ディジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求項１０記載のディジタル信号再生装置。
【請求項１６】前記ディジタル信号は、所定長のパケット形式を有してなり、
前記再生手段は、前記ディジタル信号の各パケットに付加されて記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求項１５記載のディジタル信号再生装置。
【請求項１７】所定長のディジタル信号に、同期信号、管理情報信号を付加してセクタ形式とし、前記セクタに第１の誤り訂正符号を付加し、さらにｎ（ｎは１以上の整数）セクタ単位で第２の誤り訂正符号を付加し、前記第２の誤り訂正符号にも第１の誤り訂正符号を付加して、記録媒体上に記録されている前記ディジタル信号を再生するディジタル信号再生装置において、
前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記ディジタル信号とを再生する再生手段と、
前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、
前記鍵と再生された前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を復号化して出力する復号変換手段とを備えたことを特徴とするディジタル信号再生装置。
【請求項１８】少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、
前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力され、所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求項１７記載のディジタル信号再生装置。
【請求項１９】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情報を、再生する機能を備え、
前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、
前記復号変換手段は、入力された前記鍵を、前記更新された鍵に切り換える手段を備えたことを特徴とする請求項１７記載のディジタル信号再生装置。
【請求項２０】前記再生手段は、前記第２の誤り訂正符号を付加したｎセクタの単位の区切り目で更新されているところの、前記鍵情報を、再生していく機能を備えたことを特徴とする請求項１９記載のディジタル信号再生装置。
【請求項２１】前記再生手段は、前記記録媒体上の所定の領域に記録されている、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を再生する機能を備え、前記復号変換手段は、前記暗号フラグ情報により、再生された前記ディジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求項１７記載のディジタル信号再生装置。
【請求項２２】前記再生手段は、前記第２の誤り訂正符号を付加したｎセクタの単位の区切り目で切り換えられているところの、前記暗号フラグを、再生していく機能を備えたことを特徴とする請求項２１記載のディジタル信号再生装置。
【請求項２３】ディジタル信号が記録されているディジタル信号記録媒体において、
鍵情報に所定の演算を行って得られた鍵で暗号化された前記ディジタル信号と共に、前記鍵情報が、所定の領域に記録されていることを特徴とするディジタル信号記録媒体。
【請求項２４】前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項２３記載のディジタル信号記録媒体。
【請求項２５】前記鍵情報が所定間隔で更新され、所定の領域に記録されていることを特徴とする請求項２３記載のディジタル信号記録媒体。
【請求項２６】ディジタル信号を変換するための複数種類の鍵を発生する鍵発生手段と、
前記鍵を用いてディジタル信号を変換し、変換後の変換ディジタル信号を出力する変換手段と、
前記鍵および前記変換ディジタル信号を記録媒体に記録する記録手段と、
を備えてなることを特徴とするディジタル信号記録装置。

【請求項２７】複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録された媒体が用いられ、
前記変換ディジタル信号および前記鍵を前記媒体から再生し、出力する再生手段と、
前記再生手段からの出力が入力され、前記変換ディジタル信号を前記鍵を用いて復号変換する復号変換手段と、を備えてなるディジタル信号再生装置
【請求項２８】複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録された記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ディジタル信号を記録媒体に記録再生するディジタル信号記録装置、再生装置、および記録媒体に関し、特に記録媒体上のディジタル信号の著作権を保護する機能を有するディジタル信号記録装置、再生装置、および記録媒体に関する。
【０００２】
【従来の技術】近年、ディジタル技術を用いた映像、音声等のデータ圧縮の研究が進み、これらデータの蓄積、伝送が容易にできるようになった。これに伴い、放送の分野においてもディジタル化が急速に進められている。
【０００３】例えば、アナログ映像信号、音声信号をＭＰＥＧ（Moving Picture Experts Group）規格を用いて高能率にディジタル圧縮符号化し、衛星や同軸ケーブルを通して放送するシステムが知られている。このディジタル放送を受信するための装置として、セットトップボックスと呼ばれるディジタル放送受信機がある。
【０００４】また、家庭用の映像信号、音声信号記録再生機器としては、磁気テープを用い、ディジタルＴＶ放送などのディジタル圧縮符号化された映像信号及び音声信号をディジタル信号のまま記録し再生できるディジタルＶＴＲの開発が進められている。
【０００５】このディジタル放送受信機とディジタルＶＴＲは、ディジタルインターフェースで接続され、受信したディジタル放送を高品質で保存可能となる。
【０００６】さらに、光ディスクやハードディスクを用い、映像信号及び音声信号を記録し再生する装置の開発が進められている。
【０００７】複数の情報が多重されて伝送されてくるディジタル信号を受信して所望の番組を選択する技術が、日本特開平８－５６３５０号に述べられている。また、回転磁気ヘッドを用いたディジタルＶＴＲについては、例えば、日本特開平５－１７４４９６号に記載されている。
【０００８】さらに、ディジタル放送受信機とディジタルＶＴＲをディジタルインターフェースで接続したディジタル放送記録システムについて、アイイーイーイートランザクションス　オン　コンシューマー　エレクトロニクス、第４２巻３号、１９９６年８月、６１７～６２２頁（IEEE Transactions on Consumer Electronics, Vol. 42, No. 3, August 1996, p617～622 「Newly Developed D-VHS Digital Tape Recording System for the Multimedia Era」）に詳しく述べらている。
【０００９】
【発明が解決しようとする課題】しかしながら、ディジタル放送等をディジタルＶＴＲ等で記録した、記録媒体上のディジタル信号の著作権の防衛については何ら考慮されていない。
【００１０】本発明の目的は、記録媒体上のディジタル信号の著作権を保護することにある。
【００１１】
【課題を解決するための手段】本発明は、ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力する。
【００１２】
【発明の実施の形態】以下、本発明の実施例を図面を用いて説明する。
【００１３】図１はディジタル放送受信機とディジタル信号記録再生装置を含む構成図である。２００はディジタル信号記録再生装置、２０１はディジタル放送受信装置、２０２はアンテナ、２０７は受像機である。また、２０３はチューナ、２０４は選択回路、２０５は復号回路、２０６はインターフェース回路、２０８はディジタル放送受信機２０１の動作の制御を行う制御回路である。ここで、ディジタル放送受信機２０１とディジタル信号記録再生装置２００は別体の構成で表示されているが、一体の構成となっていてもよい。
【００１４】図２は図１のディジタル信号記録再生装置２００の構成図である。図２は記録再生兼用の装置であるが、記録と再生が独立していても同様である。１００は回転ヘッド、１０１はキャプスタン、１０２ａは記録時の記録信号の生成等を行う記録信号処理回路、１０２ｂは再生時の再生信号の復調等を行う再生信号処理回路、１０４は記録再生モード等の制御を行う、例えば、マイクロプロセッサのような制御回路、１０５は回転ヘッド１００の回転等の基準となるタイミング信号を生成するタイミング生成回路、１０６は回転ヘッド及びテープの送り速度を制御するサーボ回路、１０７は記録信号の入力または再生信号の出力を行う入出力回路、１０９は記録時のタイミングを制御するタイミング制御回路、１１０は基準クロックを生成する発振回路、１１１はテープ、１１２はアナログ映像信号の記録再生回路、１１５はディジタル信号記録時のデータ暗号回路、１１６はディジタル信号再生時のデータ復号回路、１１７は、ディジタル情報を暗号あるいは復号する際にデータ暗号回

路１１５あるいはデータ復号回路１１６に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、１１８はディジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるブロック鍵を発生するブロック鍵発生器、１１９は記録時のパケットデータへのタイムスタンプ処理、再生時のパケットデータの出力制御を行う入出力制御回路である。

【００１５】ディジタル映像圧縮信号は、パケット形式のデータで、複数チャンネルの信号が時分割多重されて伝送される。図１において、アンテナ２０２で受信されたディジタル放送信号は、チューナ２０３で復調され、その後、選択回路２０４で必要なディジタル圧縮映像信号が選択される。選択されたディジタル圧縮映像信号は、復号回路２０５で通常の映像信号に復号されて、受像機２０７に出力される。また、受信信号にスクランブル等の処理が行われているときは、選択回路２０４においてそれを解除した後に、復号処理が行なわれる。受信したディジタル放送信号の記録を行うときは、選択回路２０４において記録するディジタル圧縮映像信号及びそれに関連した情報が選択され、インターフェース回路２０６を介してディジタル信号記録再生装置２００の入出力端子１０８より、ディジタル信号記録装置２００に入力され、記録される。また、記録したディジタル放送信号の再生を行うときは、ディジタル信号記録再生装置２００で再生されたディジタル圧縮映像信号等が、入出力端子１０８よりインターフェース回路２０６に出力される。インターフェース回路２０６に入力されたディジタル圧縮映像信号等は、選択回路２０４、復号回路２０５により、通常の受信時と同様の処理を行って、受像機２０７に出力する。

【００１６】図１のディジタル信号記録再生装置２００の構成を示す図２において、記録時には、入出力端子１０８より入力されたパケットデータの一部が、入出力回路１０７を介して制御回路１０４に入力される。制御回路１０４では、パケットデータに付加されている情報あるいはパケットデータとは別に送られてきた情報によりパケットデータの種類等を検出し、検出結果によって記録モードを判断し、記録信号処理回路１０２ａ及びサーボ回路１０６の動作モードを設定する。次に入出力回路１０７は、記録するパケットデータをデータ暗号回路１１５に出力する。データ暗号回路１１５では、デバイス鍵発生器１１７およびブロック鍵発生器１１８により発生される鍵をもとに制御回路１０４において生成されるデータ鍵によって、入力されたパケットデータを暗号化し、これを入出力制御回路１１９に出力する。入出力制御回路１１９では、タイミング生成回路１０５からの時間情報をもとに、入力されたパケットデータにタイムスタンプを施し、これを記録信号処理回路１０２ａに出力する。記録信号処理回路１０２ａでは、制御回路１０４で判断された記録モードに応じて、誤り訂正符号、ＩＤ情報、サブコード、暗号化に使用したブロック鍵情報等を含む記録データの生成を行い且つ記録信号を生成して、回転ヘッド１００によりテープ１１１に記録する。

【００１７】再生時には、まず任意の再生モードで再生動作を行い、再生信号処理回路１０２ｂでＩＤ情報を検出する。そして、制御回路１０４でどのモードで記録されたかを判断し、再生信号処理回路１０２ｂ及びサーボ回路１０６の動作モードを再設定して再生を行う。再生信号処理回路１０２ｂでは、回転ヘッド１００より再生された再生信号より、同期信号の検出、誤り検出訂正、ブロック鍵情報等の取得を行い、パケットデータを再生して入出力制御回路１１９に出力する。入出力制御回路１１９では、タイミング生成回路１０５で生成されたタイミングを基準としてタイムスタンプを取り除いたパケットデータをデータ復号回路１１６に出力する。データ復号回路１１６では、デバイス鍵発生器１１７により発生される鍵、および再生によって得られたブロック鍵をもとに、制御回路１０４において生成されるデータ鍵によって復号して、入出力回路１０７に出力する。

【００１８】記録時には、入出力端子１０８より入力された記録データのレートを基準としてタイミング制御回路１０９により記録再生装置の動作タイミングを制御し、再生時には、発振回路１１０により発振されたクロックを動作基準として動作する。

【００１９】図３はディジタル映像圧縮信号のパケットの構成図である。１パケットは固定長、例えば、１８８バイトで構成されており、４バイトのパケットヘッダ３０６と、１８４バイトのパケット情報３０７により構成されている。ディジタル圧縮映像信号は、パケット情報３０７の領域に配置される。また、パケットヘッダ３０７はパケット情報の種類等の情報により構成される。

【００２０】図４は図３のパケットヘッダ３０６の構成図である。５０１はパケットの先頭を示す同期バイト、５０２は誤りの有無を示す誤り表示、５０３はユニットの開始を示すユニット開始表示、５０４はパケットの重要度を示すパケットプライオリティ、５０５はパケットの種類を示すパケットＩＤ、５０６はスクランブルの有無を示すスクランブル制御、５０７は追加情報の有無及びパケット情報の有無を示すアダプテーションフィールド制御、５０８はパケット単位でカウントアップされる巡回カウンタである。

【００２１】図５はディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。７１は図３のパケットである。通常、上記映像信号に音声信号、プログラムに関する情報等が付加され、複数チャンネルのプログラムが時分割多重されて伝送される。

【００２２】図５（ａ）は、３チャンネルのプログラムを多重した例であり、Ｖ１、Ｖ２、Ｖ３はそれぞれのチャンネルの映像信号、Ａ１、Ａ２、Ａ３はそれぞれのチャンネルの音声信号のパケットである。なお、映像また

は音声は、一つのチャンネルに複数の映像または音声で構成されている場合もある。Ｐ０、Ｐ１、Ｐ２、Ｐ３はプログラムに関する情報である。それぞれのパケットは、異なるパケットＩＤ５０５が割り当てられており、これによりパケットの内容を識別することができる。

【００２３】Ｐ０は、図５（ａ）の伝送信号全体に関する情報であり、それぞれのプログラムにどのパケットＩＤが割り当てられているかを認識するためのプログラムアソシエーションテーブル、番組ガイド情報等のパケットが時分割多重されて伝送される。Ｐ１、Ｐ２、Ｐ３は、それぞれのプログラムに関する情報であり、そのチャンネルの映像パケット、音声パケット等にどのパケットＩＤが割り当てられているかを認識するためのプログラムマップテーブル、スクランブル情報等のパケットが時分割多重されて伝送される。通常、プログラムアソシエーションテーブルのパケットＩＤは決まった値、例えば０が割り当てられている。

【００２４】受信時には、まずプログラムアソシエーションテーブルによって受信したいプログラムのプログラムマップテーブルにどのパケットＩＤが割り当てられているかを認識し、次に、受信したいプログラムのプログラムマップテーブルによって映像パケット、音声パケット等にどのパケットＩＤが割り当てられているかを認識する。そして、映像パケットおよび音声パケットを抽出してディジタル圧縮データの復号を行う。また、同時にプログラムクロックリファレンスを抽出し、これによってディジタル圧縮データの復号回路の復号タイミングが符号化時のタイミングと同期するように復号回路の動作を制御する。

【００２５】ＣＲは、ディジタル圧縮データの復号時の同期をとるためのプログラムクロックリファレンス情報である。

【００２６】もちろん、多重するチャンネル数は３チャンネル以外、例えば４チャンネルでもよいし、また、これ以外の情報を多重してもよい。

【００２７】図５（ｂ）は、図５（ａ）から第１のチャンネルの情報およびそれに関連したプログラム情報のみを選択したものである。第１のチャンネルを記録する場合には、この情報をディジタル放送受信機２０１から記録再生装置２００に出力する。もちろん、これ以外の情報を含めて記録してもよいし、また、再生時の処理をやりやすくするために、パケットの情報の一部を変更してもよい。例えば、プログラムアソシエーションテーブルの情報を記録するプログラムのみの情報に変更すれば、再生時にチャンネルの選択が不要になる。

【００２８】図６は図２のデータ暗号回路１１５の構成図である。１１５１はパケットデータ入力端子、１１５７はパケットデータ出力端子、１１５３ａ、１１５３ｂはデータ鍵入力端子、１１５３ｃはデータ鍵選択信号入力端子、１１５３ｄは、処理モード選択信号入力端子、１１５２、１１５６はブロック処理回路、１１５４は鍵スケジュール回路、１１５５は暗号器、１１５８ａ，１１５８ｂはデータ鍵レジスタ、１１５９はデータ鍵セレクタである。データ暗号回路１１５は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で暗号化して出力する。この際、このデータ鍵をある時間間隔で変更していくことにより、テープ上に記録されるパケットデータの安全性を高めることができる。

【００２９】暗号器１１５５は、例えば、伝送中にビット誤り等のエラーが発生しても、そのエラーが後続のデータに影響を与えない、すなわちエラー伝播がないように、複数ビットで構成されるブロックを単位として暗号処理を簡単な回路構成で実現できるブロック暗号を用いる。

【００３０】入力端子１１５１から入力されたパケットデータは、まず、ブロック処理回路１１５２において、複数ビットからなるブロックＰに区切られる。例えば１ブロックを６４ビットとする。各ブロックは、暗号器１１５５において順次暗号化され、その結果ブロックＣを出力し、ブロック処理回路１１５６において、今度はブロックをパケットデータの形式に戻して出力端子１１５７へ出力する。ここで、暗号化のための鍵であるデータ鍵は、制御回路１０４より、データ鍵入力端子１１５３ａおよび１１５３ｂから入力され、データ鍵レジスタ１１５８ａ、１１５８ｂに記憶される。例えば、データ鍵レジスタ１１５８ａには、現在のデータ鍵を、データ鍵レジスタ１１５８ｂには次に切り換えるデータ鍵を記録させる。

【００３１】また、データ鍵選択信号入力端子１１５３ｃからは、制御回路１０４より、データ鍵レジスタ１１５８ａ、１１５８ｂのどちらのデータ鍵を選択するかを示す信号が入力され、データ鍵セレクタ１１５９により、選択されたデータ鍵が出力される。ここでは、例えば鍵レジスタ１１５８ａのデータ鍵が選択されているものとする。選択されたデータ鍵は、スケジュール回路１１５４においてサブ鍵ＫＡ、ＫＢに変換され、暗号器１１５５に供給される。例えば、データ鍵の長さ５６ビット、サブ鍵の長さが、それぞれ３２ビットとし、データ鍵の上位３２ビットをＫＡに割り当て、データ鍵の上位３２ビットと下位３２ビットの加算値をＫＢに割り当てる。

【００３２】ここで、データ鍵を変更する場合には、制御回路１０４より、データ鍵レジスタ１１５８ｂを出力するようデータ鍵選択信号入力端子１１５３ｃから信号が入力される。データ鍵セレクタは、一つのパケットデータのブロック全ての暗号化が終了するまでは、その選択出力を切り換えず、次のパケットデータとの間で切り換えるよう制御する。

【００３３】その他、例えば、暗号器１１５５の出力と、暗号器１１５５の入力を排他的論理和をとり、ブロ

ック単位でフィードバックをかけることで、暗号強度を増す方法もある。

【００３４】図７は図６の暗号器１１５５の構成図である。同図中、５５１、５５２、５５３、５５４は暗号処理部、Ｐａ、Ｐｂは入力ブロックデータＰの上位および下位ビット、Ｃａ、Ｃｂは暗号化されたデータ、ＫＡ、ＫＢは、サブ鍵である。同図に示すように、例えば入力された６４ビットのブロックＰを、その上位３２ビットＰａと下位３２ビットＰｂに分離する。そのＰａ、Ｐｂは、暗号処理部５５１において、排他的論理和（５５１１）、ビットシフトおよび加算演算（５５１２、５５１３、５５１５：Ａ＜＜＜ｐは、Ａをｐビット左方向に循環ビットシフトすることを表す）、加算演算（５５１４、５５１６）を行い、その結果を暗号処理部５５１と同様の処理を行う後続の暗号処理部５５２、５５３、さらに図示しない暗号処理部に入力して複数段繰り返し演算を行い、最終段の暗号処理部５５４により出力されたデータＣａ、Ｃｂより、暗号化されたブロックＣを得る。

【００３５】以上は、図２、図７のデータ暗号回路１１５について説明したが、図２のデータ復号回路１１６では、暗号器１１５５の逆の流れで演算していくことにより、暗号化されたブロックを復号することができる。ただし、図７の演算５５１６は、減算処理とする。また、当然、サブ鍵ＫＡ、ＫＢは、暗号時と同一の鍵を用いなければならない。

【００３６】その他、記録するパケットデータを保護する必要が無い場合、例えば記録する番組が自由にコピーしてもよいよう許可されている場合、パケットデータを暗号化しないで、そのままテープ上に記録する場合がある。これは例えば、データ暗号回路１１５、データ復号回路１１６を、入力パケットの暗号・復号の機能と、なにもしないで通過させる機能とを切り換えることで実現できる。図２、図６のデータ暗号回路１１５において、図６の処理モード選択信号入力端子１１５３ｄを介して入力される処理モード選択信号により、図７の演算５５１６への入力Ｘ５を、図示していないが、零に固定することで、暗号、復号処理を行わずに、ブロックを通過させることが出来る。この方法によれば、入力パケットの通過遅延時間を一定に保ったまま、動作を切り換えることができる。また、図示しないが、他の方法としては、入力端子１１５１から入力されたパケットデータを、ブロック処理回路１１５２、暗号器１１５５、ブロック処理回路１１５６を介さず、出力端子１１５７に出力するか、ブロック処理回路１１５６から出力されるパケットデータを出力端子１１５７に出力するかを切り換える切り換え回路を出力端子１１５７の前段に設け、処理モード選択信号入力端子１１５３ｄを介して入力される処理モード選択信号をその切り換え回路に入力して、ブロック処理回路１１５６から出力されるパケットデータか、入力端子１１５７に入力されたパケットデータかを切り換える方法もある。これらの方法は、図２、図１９のデータ復号回路１１６においても前述と同様の構成で実現できる。

【００３７】図８は図２のデータ暗号回路１１５、データ復号回路１１６に供給するデータ鍵の生成例を示すところの制御回路１０４内のデータ鍵の生成図である。デバイス鍵発生器１１７は、例えば９６ビットのあらかじめ定められた固定の鍵情報を記憶している。ブロック鍵発生器１１８は、例えば図２の制御回路１０４からの司令１１８１により、９６ビットの乱数を発生させる乱数発生器である。１２０は９６ビットの排他的論理和演算器、１２１はハッシュ関数演算器である。図８（ａ）では、ブロック鍵とデバイス鍵は、排他的論理和演算器１２０で排他的論理和がとられ、ハッシュ関数演算器１２１にてハッシュ演算がなされ、その結果のうちの選択された５６ビットが、データ鍵として図２のデータ暗号回路１１５に供給される。ハッシュ関数は、その出力結果から、入力データが類推困難な関数であり、データ鍵から、秘密情報であるブロック鍵、デバイス鍵が求められない。

【００３８】また、図２の制御回路１０４からの司令１１８１をある時間間隔で発生させ、上述の演算によるデータ鍵生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、記録媒体上のデータの安全性を高めることが可能となる。次に、ブロック鍵発生器１１８で発生されたブロック鍵（Ｋｒ）は、図２の記録信号処理回路１０２ａに送られ、テープ１１１上に記録される。

【００３９】再生時には、ブロック鍵発生器１１８の発生するブロック鍵の代わりに、テープ１１１上から再生されたブロック鍵（Ｋｐ）を用いて、上記と同様の演算を行い、データ鍵を得、図２のデータ復号回路１１６に供給される。

【００４０】図８（ｂ）は、テープ１１１上に記録する鍵情報Ｋｒとして、ブロック鍵をデバイス鍵で排他的論理和演算したものを用いる例である。この場合、ハッシュ関数演算器にはブロック鍵そのものが入力される。再生時には、図８（ａ）中のブロック鍵の代わりに、テープ１１１上から再生されたＫｐを用いて、上記と同様の演算を行い、データ鍵を得、データ復号回路１１６に供給される。

【００４１】次に、テープへの記録方法について述べる。

【００４２】図９は、１トラックの記録パターンである。３は時間情報、プログラム情報等のサブコードを記録するサブコード記録領域、７はディジタル圧縮映像信号を記録するデータ記録領域、２及び６はそれぞれの記録領域のプリアンブル、４及び８はそれぞれの記録領域のポストアンブル、５はそれぞれの記録領域の間のギャ

ップ、１及び９はトラック端のマージンである。このように、各記録領域にポストアンブル、プリアンブル及びギャップを設けておくことにより、それぞれの領域を独立にアフレコを行うことができる。もちろん、記録領域７にはディジタル圧縮映像信号以外のディジタル信号を記録してもよい。データ記録領域７は、複数のブロック（前述の暗号化の小単位であるブロックとは異なる）により構成されている。

【００４３】図１０は図９のデータ記録領域７のブロックの構成図である。２０は同期信号、２１はＩＤ情報、２２はデータ、２３は第１の誤り検出訂正のためのパリティ（Ｃ１パリティ）である。例えば、同期信号２０は２バイト、ＩＤ情報２１は３バイト、データ２２は９９バイト、パリティ２３は８バイトで構成されており、１ブロックは１１２バイトで構成されている。

【００４４】図１１は図１０のＩＤ情報２１の構成図である。３１はグループ番号、３２はトラックアドレス、３３は１トラック内のブロックアドレス、３５はグループ番号３１、トラックアドレス３２及びブロックアドレス３３の誤りを検出するためのパリティである。ブロックアドレス３３は、各記録領域でのブロックの識別を行うためのアドレスである。例えば、図９のデータ記録領域７では０～３３５とする。トラックアドレス３２は、トラックの識別を行うためのアドレスであり、例えば、１トラックまたは２トラック単位でアドレスを変化させ、ｎトラックを識別することが出来る。例えば、０～５または０～２とすることにより、６トラックを識別することができる。図１１のグループ番号３１は、例えば、トラックアドレス３２で識別する６トラック単位で変化させ、０～１５とすることにより、９６トラックを識別することができる。トラックアドレス３２は、後述する第２の誤り訂正符号の周期と同期させておけば、記録時の処理及び再生時の識別を容易にすることができる。

【００４５】図１２は図９のデータ記録領域７の１トラック分のデータの構成図である。なお、図１０に図示の同期信号２０およびＩＤ情報２１は省略してある。データ記録領域７は、例えば、３３６ブロックで構成されており、最初の３０６ブロックにデータ４１を、次の３０ブロックに第２の誤り訂正符号（Ｃ２パリティ）４３を記録する。Ｃ２パリティ４３は、ｎトラック単位、例えば６トラック単位で構成されている。６トラック単位でみると、データは３０６ブロック×６トラックのデータであり、そのデータを１８分割して、それぞれの１０２ブロックに、１０ブロックのＣ２パリティを付加する。誤り訂正符号は、例えばリードソロモン符号を用いればよい。各ブロック９９バイトのデータは、３バイトのヘッダ４４と９６バイトのデータ４１により構成されている。

【００４６】図１３は、１８８バイトのパケット形式で伝送されたディジタル圧縮映像信号を、図１２のデータ４１に記録する時の１パケットのブロックの構成例である。この場合には、４バイトの時間情報２５を付加して１９２バイトとし、２ブロックに１パケットを記録する。時間情報２５は、パケットの伝送された時間の情報である。すなわち、パケットの先頭が伝送された時の時間またはパケット間の間隔を基準クロックでカウントし、そのカウント値をパケットデータと共に記録しておき、再生時にその情報を基にしてパケット間の間隔を設定することにより、伝送された時と同一の形でデータを出力することができる。

【００４７】図１４は図１２のデータ記録領域７のヘッダ４４の構成図である。ヘッダ４４は、フォーマット情報４５、ブロック情報４６および付加情報４７により構成される。フォーマット情報４５、およびブロック情報４６には、記録に関する様々な記録情報が、また付加情報４７には、その他補助的な情報が記録される。

【００４８】フォーマット情報４５は、記録フォーマットに関する情報であり、記録モード（標準速モードその他の識別）、取り扱うパケットデータの種類、記録されているパケットデータがコピー可能か否か等を示すコピー制限情報等が格納され、複数のブロックで、１つの情報を構成する。例えば１２ブロックの１２バイトで１つの情報を構成している。そして、この情報を複数回繰り返し多重記録することにより、再生時の検出能力を向上させている。ここに、前述の鍵情報等をも記録しておくことが可能である。

【００４９】ブロック情報４６は、データ記録領域４１に記録されるデータの種類を識別するための情報である。ここには、高速可変速再生用データの有無、種類（どの速度に対応した高速可変速再生用データであるか）等を記録しておく。ここに、前述の鍵情報等をも記録しておくことも可能である。

【００５０】付加情報４７は、例えば、６ブロックの６バイトで一つの情報であるパックデータを構成し、最初の１バイトが情報の種類を表すアイテムコード、残りの５バイトをデータとすることにより、いろいろな種類のデータを記録することができる。例えばここに前述のブロック鍵等の鍵情報や、その他、記録時間等の情報や記録信号の種類等を記録しておくことができる。

【００５１】図１５は図１４の付加情報４７の領域に、ブロック鍵を格納する場合のパックデータの構成図である。

【００５２】パックデータの最初の１バイトには後続の情報が鍵情報であることを示すアイテム情報コードを格納する。

【００５３】２バイト目には、格納されている鍵の種類を示す情報（鍵シーケンス番号、鍵属性、鍵フラグ）を記録する。前述のように、ブロック鍵をある時間間隔で順次変更していくことで、記録媒体上のデータの安全性

を高めることができるので、例えば、このパックに格納されているブロック鍵が、現在のパケットデータの暗号化に用いられるブロック鍵か、次に用いるブロック鍵かを示す鍵属性情報を記録しておく。また、ブロック鍵が更新される度に反転する鍵フラグで、切り換えタイミングを記録する。この情報により再生時の鍵の切り換えをスムーズにする。また、鍵シーケンス番号には、一つのパックでブロック鍵が格納できない場合、後続のパックがあることを示す情報を格納する。例えばブロック鍵が９６ビットの場合、３つのパックに分割して格納し、それぞれの鍵シーケンス番号には、２、１、０を格納し、０が最終パックであることを示す。その他、全体のデータのサイズを格納しておき、残りの大きさを知る方法もある。

【００５４】３バイト目から６バイト目に、ブロック鍵を収納する。

【００５５】前述の図８（ｂ）の例では、鍵情報Ｋｒがブロック鍵の代わりに格納される。

【００５６】図１６はブロック鍵の格納方法を示す図である。この例は、各トラックのパックデータには、現在の鍵情報のみを記録する場合である。したがって、前述の鍵属性は、現在の鍵を示すのみの固定情報であり、記録しなくてもよい。同図中（１）は、９６ビットの現在のブロック鍵Ａ（Ａ０乃至Ａ１１）が３個のパックに分割して格納される状態を示す。通常、これらのパックは、データの信頼性の向上のため、一つのトラックにつき、複数回記録される。例えば、３個のパックをトラックの最初、半ば、最後のそれぞれの領域に記録する（計９個）ことで、磁気ヘッドの目詰まり等による、再生信号のバースト欠落の影響を軽減できる。また、３個のパックは必ずしも連続したパックとして記録する必要はなく、各パックの間に他の情報を格納したパックを挿入し、鍵情報を格納しているパックを分散して記録することで、鍵情報自身の保護も可能となり、さらに信頼性が向上する。同図（２）はブロック鍵がＢに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Ｂの鍵フラグは反転している。

【００５７】図１７はブロック鍵の他の格納方法を示す図である。図１７は、現在の鍵情報と共に、次に使用する鍵情報もあらかじめ発生させておき記録する方法である。ここで、鍵属性情報は、現在のパケットデータの暗号化に用いられるブロック鍵の場合“０”、次に用いるブロック鍵の場合“１”とする。また、ブロック鍵が更新される度に反転する鍵フラグは“０”と“１”を交互に繰り返す。

【００５８】同図中（１）は、９６ビットの現在のブロック鍵Ａが格納される状態を示す。（２）には、次のブロック鍵Ｂが格納される。この（１）および（２）が、同一のトラック内のブロックの付加情報エリアに記録される。（３）は、ブロック鍵がＢに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Ｂは、鍵属性情報“０”の現在の鍵に、また、鍵フラグも反転している。さらに（４）は、次に用いる鍵Ｃが格納される。（３）および（４）が、同一のトラック内のパックデータとしてトラックに記録される。

【００５９】ブロック鍵の更新タイミングを示す鍵フラグの格納場所としては、付加情報４７のパックに格納する以外に、前述の図１４に示したフォーマット情報４５、あるいはブロック情報４６に格納する方法もある。

【００６０】以上のように、鍵情報が、テープ上に記録されるが、ブロック鍵を切り換えるタイミングとしては、前述のＣ２パリティの付加の単位であるｎトラック（本実施例では６トラック）の区切り目とすることで、再生時に、Ｃ２パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【００６１】また、以上の例ではブロック鍵が更新されるタイミングを示す情報を鍵フラグとして記録したが、図２の記録信号処理回路１０２aにおいて、前述の図１１に示したトラックアドレス３２、あるいはグループ番号３１の値と、Ｃ２パリティの演算の周期および更新のタイミングを同期させることで、特に鍵フラグを記録しなくとも、再生時における鍵情報の更新のタイミングを、このトラックアドレス３２あるいはグループ番号３１の値で検出することも可能である。例えば、図２の記録信号処理回路１０２aにおいて、トラックアドレス３２が、トラック１本毎に０から５の値を繰り返し、その値０から５の６本のトラックを、前述のＣ２パリティの付加の単位とする。そして、値が５から０になるタイミングで、データ暗号回路１１５において、ブロック鍵を更新して、記録する。再生時においては、図２の再生信号処理回路１０２bにおいて、このトラックアドレス３２の値が５から０になるタイミングを検出し、データ復号回路１１６において、鍵を更新していけばよい。また、さらに長い周期で更新する場合には、例えば、グループ番号３１を用いて、トラックアドレス３２の値が５から０になる際に、グループ番号３１を１増加させ、０から１５の値を繰り返すようにすることで、９６トラックの単位で、しかもＣ２パリティの付加の単位の区切り目の、更新のタイミングを検出することが可能となる。

【００６２】図１８は図１３の時間情報２５（４バイト＝３２ビット）の具体的構成例であり、鍵フラグ、暗号フラグ格納の他の方法を示したものである。ここでは、例えば、時間情報２５１としては、２２ビットの情報であり、２５２は前述の鍵フラグ（１ビット）、２５３は、後続のパケットデータが暗号化されているかどうかを示す暗号フラグ（１ビット）である。記録時には、図２の入出力制御回路１１９は、タイムスタンプである時間情報２５１とともに、暗号フラグ２５３に、後続のパケットデータが暗号化されている場合には例えば“１”を、暗号化されていない場合には“０”を格納し、ま

た、鍵フラグ２５２には、後続のパケットデータに対応する前述の鍵情報を格納するパックデータの鍵フラグを格納する。再生時には、図２の入出力制御回路１１９において、記録時に付加した時間情報２５を取り除いてデータ復号回路１１６に出力するとともに、暗号フラグ２５３、鍵フラグ２５２をデータ復号回路１１６に供給し、データ復号回路１１６の動作を制御する。

【００６３】図１９は図２のデータ復号回路１１６の構成図である。１１６１はパケットデータ入力端子、１１６７はパケットデータ出力端子、１１６３ａ、１１６３ｂはデータ鍵入力端子、１１６３ｃはデータ鍵選択信号入力端子、１１６３ｄは、処理モード選択信号入力端子、１１６２、１１６６はブロック処理回路、１１６４は鍵スケジュール回路、１１６５は復号器、１１６８ａ，１１６８ｂはデータ鍵レジスタ、１１６９はデータ鍵セレクタである。データ復号回路１１６は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で復号化して出力する。

【００６４】復号器１１６５は、複数ビットで構成されるブロックを単位として復号処理を実現するブロック暗号を用いる。

【００６５】入力端子１１６１から入力されたパケットデータは、データ暗号回路１１５と同様に、複数ビットからなるブロックＣに区切られ、各ブロックは、復号器１１６５において順次復号化され、その結果ブロックＰを出力し、ブロック処理回路１１６６において、パケットデータの形式に戻して出力端子１１６７へ出力する。ここで、復号化のための鍵であるデータ鍵は、制御回路１０４より、データ鍵入力端子１１６３ａおよび１１６３ｂから入力され、データ鍵レジスタ１１６８ａ、１１６８ｂに記憶される。例えば、データ鍵レジスタ１１６８ａには、現在のデータ鍵を、データ鍵レジスタ１１６８ｂには次に切り換えるデータ鍵を記録させる。

【００６６】また、処理モード選択信号入力端子１１６３ｄからは、入出力制御回路１０９より検出した暗号フラグ２５３が入力され、復号器１１６５を復号動作のモードか、何もしないで通過させるモードかを決定する。さらに、データ鍵選択信号入力端子１１６３ｃからは、入出力制御回路１０９より検出した鍵フラグ２５２が入力され、データ鍵セレクタ１１６９により、選択されたデータ鍵が出力される。選択されたデータ鍵は、スケジュール回路１１６４においてサブ鍵ＫＡ、ＫＢに変換され、暗号器１１６５に供給される。

【００６７】ここで、図２の入出力制御回路１１９で検出した、暗号フラグ、あるいは鍵フラグが変化すると、それに連動して、データ復号器１１６の動作モード、データ鍵の選択が行われる。

【００６８】以上のように、各パケットデータへ暗号フラグ、鍵フラグを付加することにより、パケットデータ単位での、暗号化の有無、鍵情報の判別、および復号処理が実現できる。

【００６９】その他、暗号化されているかどうかを示す暗号フラグの格納場所としては、図１５に示した鍵情報を格納するパックの２バイト目に格納する方法、あるいは前述の図１４に示したフォーマット情報４５、ブロック情報４６に格納する方法もある。

【００７０】暗号フラグをフォーマット情報４５、あるいはブロック情報４６等に格納することで、例えば暗号フラグが“１”を示す時、すなわちパケットデータが暗号化されている場合には、データ復号回路１１６の動作を復号動作とするとともに、付加情報４７の鍵情報を格納するパックから、鍵情報を取得するようにし、暗号フラグが“０”の場合は、データ復号回路１１６の動作を、復号しないでそのまま出力するようにすることで、パケットデータが暗号化されていない場合の制御動作の簡略化が図れる。また、暗号フラグを鍵情報を格納するパックに格納する方法では、暗号フラグが“０”、すなわちパケットデータが暗号化されていない場合は、そのパックの３バイト目以降のブロック鍵情報は格納されていない。

【００７１】その他、暗号フラグを用いずに、例えば、鍵情報を格納するパックの有無で暗号化されているかどうかを判別することもできる。

【００７２】図２０は図２の記録信号処理回路１０２ａおよび再生信号処理回路１０２ｂからなるディジタル記録再生信号処理回路１０２の構成図である。４００はメモリ回路、４０１は図２の制御回路１０４に従いメモリ回路４００を制御するアドレス等を生成するメモリ制御回路、４０２はＣ２パリティ演算回路、４０３はＣ１パリティ演算回路、４０４は前記制御回路１０４からの設定内容に従い記録時のＩＤ情報、サブコード生成、フォーマット情報、ブロック情報、鍵情報等の付加情報の付加、および再生時のＩＤ情報、サブコード、フォーマット情報、ブロック情報、鍵情報等の付加情報の取得等を行う付加情報処理回路、４０５は記録時の変調処理及び再生時の復調処理を行う変復調回路である。本実施例では、一例としてＣ２パリティ演算を行うために６トラックのデータを必要とするため、メモリ回路４００は少なくとも６トラック分のデータを蓄積する容量を備えるものとする。

【００７３】記録時には、端子４１１、４１３を介して図２の制御回路１０４により、記録状態に設定される。図２のデータ暗号回路１１５で暗号化されたパケットデータが端子４１０から入力され、メモリ制御回路４０１の制御信号に従いメモリ回路４００に蓄積される。Ｃ２パリティ演算に必要なデータが蓄積された後、メモリ回路４００から逐次読みだされ、Ｃ２パリティ演算回路４０２に入力されて、所定の演算が行われる。Ｃ２パリティ演算回路４０２で得られた演算結果は、メモリ回路４００に蓄積される。一方、端子４１３を介して図２の制

御回路１０４からの設定に従い、付加情報処理回路４０４で、入力された暗号化パケットデータの鍵に対応した鍵情報等のパックデータが生成され、メモリ回路４００に蓄積される。さらに前記した記録ブロックを構成するように、鍵情報等を含めメモリ回路４００から読みだされたデータは、Ｃ１パリティ演算回路４０３でＣ１パリティを付加され、変復調回路４０５に入力される。変復調回路４０５で所定の変調処理された信号は、端子４１４を介して出力され、図２の記録再生アンプ１１６、回転ヘッド１００を介してテープ１１１上に記録される。

【００７４】図２１はデータ記録開始時における信号処理のタイミングを示す図である。図２１（ａ）はデータ暗号化回路１１５から入力されるパケットデータ、図２１（ｂ）は、データ暗号化回路１１５が暗号化の際に用いたデータ鍵、図２１（ｃ）は、前述のＣ２パリテイ４３の６トラック単位構成にあわせて、図２０のＣ２パリティ演算回路４０２でのＣ２パリティ演算サイクル（本実施例では６トラック）を示し、図２１（ｄ）は回転ヘッド１００を介してテープ１１１に記録する記録信号を示している。図２１の実施例では、記録開始が設定される時間ｔ１より前にあらかじめブロック鍵Ａを生成し、データ鍵Ｋａを演算して、データ暗号化回路１１５に供給しておく。また、記録開始が設定される時間ｔ１より前は、記録信号処理回路１０２ａは入力信号に関らずパケット無しとみなして記録信号処理を行うように制御する。これにより、時間ｔ０に記録開始が設定されても、期間ｐ０のデータに対してのＣ２パリティの演算は可能となる。

【００７５】図２の制御回路１０４は、時間ｔ０で記録開始にした時の入力データのＣ２パリティ演算サイクルｓ０が終了して、前記第２の誤り訂正符号を構成するｎトラック（本実施例では６トラック）の先頭から記録信号を出力する（図２１（ｄ））ように制御する。また、データ鍵は、このＣ２パリティの演算サイクルで更新される。例えば、時間ｔ２より前にブロック鍵Ｂを生成し、データ鍵Ｋｂを演算してデータ暗号化回路１１５に供給しておき、時間ｔ２の時点でデータ暗号化回路１１５においてデータ鍵をＫｂに切り換える。通常、データ暗号化回路１１５は、その処理のため、パケットデータの入力から出力までの間に遅延時間が生じる。そこで、時間ｔ２からデータ暗号化回路１１５がパケットを暗号化処理することにより生じるデータ遅延時間分前の時点で、データ暗号化回路１１５に供給するデータ鍵をＫｂに切り換える。あるいは、データ鍵が切り換えられたパケットデータからは、次の演算サイクルの処理に先送りしてもよい。この実施例では、先頭部分に余分なデータが記録されるが、記録開始にする時間ｔ１のタイミングによらず、記録すべき信号に対しＣ２パリティを付加し、上記Ｃ２パリティ演算サイクル単位で記録できる。また、再生時において、先頭の余分なデータ部分は、パケット無しとみなして記録処理しているので、Ｃ２パリティ演算に用いられるだけで、出力されることはない。

【００７６】記録終了時には、前記記録再生信号処理回路１０２ａの、テープ１１１への記録動作を、複数トラックのデータを用いて演算するＣ２パリティの演算サイクル（本実施例では６トラック）完結で行うように前記制御回路１０４で制御する。この制御方式により、記録開始、記録終了の切換えタイミングによらず、テープ１１１上の記録データに全てＣ２パリティを付加し、Ｃ２パリティの演算サイクル単位で鍵情報が更新されパケットデータが暗号化されるので、再生時には、Ｃ２パリティ演算サイクル単位で再生でき、Ｃ２パリティ演算が可能となるので、鍵情報のデータ信頼性も向上する。

【００７７】図２２は図２のテープ１１１上の鍵情報を示す図である。同図中、１１１１から１１１７は、Ｃ２パリティ演算サイクルである６トラック単位で示した記録トラックである。この図の場合、記録トラック１１１１から１１１３までが、ブロック鍵Ａ、記録トラック１１１４から１１１６までがブロック鍵Ｂをもとに暗号化されたパケットデータ、およびそれらに対応した鍵情報であるパックデータが格納される。また、記録トラック１１１７は暗号化されずに記録されたトラックである。この図のように、暗号化されたトラックと、暗号化されていないトラックが同一のテープ上に混在することも可能である。鍵情報の更新は、例えば、４８トラック、９６トラック等、ｍ×ｎトラック毎（ｍは１以上の整数、ｎは本実施例では６）、あるいは一つの番組全体等考えられるが、鍵の切り換わり目、あるいは暗号化されたトラックと、暗号化されていないトラックとの境目は、Ｃ２パリティ演算サイクル（本実施例では６トラック）の区切り目である。

【００７８】以上、記録の際の動作について説明した。ここで、鍵情報をサブコード領域（図９の７）に記録することも可能であるが、鍵情報を、各ブロックのヘッダ（図１２の４４）の部分に格納し、各トラック上のデータ記憶領域（図９の７）に記録することで、アフレコ等による鍵情報のみの書き換えは困難となる。従って、鍵情報の消失を防ぐことができ、また、故意に鍵情報のみを改ざんして意図的に暗号通信を行うことはできない効果がある。

【００７９】次に、テープからの再生方法について述べる。

【００８０】図２０のディジタル記録再生信号処理回路１０２において、再生時は、端子４１１、４１３を介して図２の制御回路１０４によって、再生状態に設定される。前記テープ１１１から回転ヘッド１００で再生され、端子４１４から入力された再生信号は、変復調回路４０５で復調処理された後、Ｃ１パリティ演算回路４０３でＣ１パリティ演算を行い、誤り検出およびその訂正を行い、Ｃ１パリティ演算結果も一緒にメモリ回路４０

０に蓄積される。Ｃ２パリティ演算に必要なデータが蓄積された後、メモリ制御回路４０１の制御信号に従いメモリ回路４００から逐次読みだされ、Ｃ２パリティ演算回路４０２に入力される。Ｃ２パリティ演算回路４０２では、上記データで演算を行い、誤りの検出、訂正処理したデータおよびＣ２パリティ演算結果を、再びメモリ回路４００に蓄積する。

【００８１】図２のタイミング生成回路１０５から端子４１２を介して入力されるタイミング信号を基準として所定の順番にメモリ回路４００からデータを読みだし、前記Ｃ１パリティ、Ｃ２パリティの演算結果を参照し、誤りの無いデータのみを端子４１０から図２の入出力制御回路１１９に出力する。一方、付加情報処理回路４０４では、メモリ回路４００から読み出したデータから鍵情報やサブコード等を取得し、端子４１３を介して図２の制御回路１０４に送出する。その後、図８で示した演算、すなわち再生によって得られた鍵情報から、Ｋｐを取り出し、デバイス鍵発生器１１７からのデバイス鍵との排他的論理和をとって、ハッシュ関数１２１の演算を行い、データ鍵を得、図２のデータ復号回路１１６に出力する。このデータ鍵は、記録時に用いたデータ鍵と同一のものであり、データ復号回路１１６において、正しくもとのパケットデータを得ることができる。

【００８２】図２３は、本発明のデータ再生時における信号処理のタイミングを示す図である。図２３（ａ）は回転ヘッド１００を介してテープ１１１から再生される再生信号、図２３（ｂ）は上記Ｃ２パリティの演算サイクル（本実施例では６トラック）を示し、図２３（ｃ）は入出力制御回路１１９から出力されるパケットデータを示し、図２３（ｄ）は、図２のデータ復号回路１１６に供給されるデータ鍵を示している。付加情報処理回路４０４では、演算サイクルｓ３においては、このサイクルで用いられている鍵情報ＫｐＣが検出されている。このＫｐＣにより前述の演算で得られたデータ鍵Ｋｃが、例えば前述のデータ鍵レジスタ１１６３ａに記憶されており、データ鍵セレクタ１１６９も、データ鍵レジスタ１１６３ａのデータ鍵Ｋｃが出力されるように選択されている。

【００８３】次に、演算サイクルｓ４において、鍵情報ＫｐＤが用いられていることが検出されると、あらかじめ、データ鍵Ｋｄを前述の演算で求めておき、データ鍵レジスタ１１６３ｂに記憶させ、時間ｔ３のタイミングで、データ鍵セレクタ１１６９を制御してデータ鍵レジスタ１１６３ｂのデータ鍵Ｋｄに切り換える。以上の方法により、データ鍵を更新しながらの再生動作が可能となる。

【００８４】また、既に記録済みのテープに追加記録する場合、Ｃ２パリティの付加単位の区切り目から、記録を開始するようにすることで、追加記録直前のトラックの鍵情報のデータ信頼性を損なわずに、つなぎ記録が可能となる。

【００８５】その他、パケットデータが暗号化されているかいないかを区別する方法としては、図４で示した同期バイト５０１は、通常固定データであるので、例えば、再生信号処理回路１０２ｂにおいて、この同期バイトの検出を行い、検出できた場合は、図２のデータ復号回路１１６を入力されるパケットデータを何もしないで通過させる機能に切り換え、検出できなかった場合は、図２のデータ復号回路１１６を復号機能の動作に切り換え、付加情報エリア内の鍵情報を検出する動作を行うことで、記録時に、パケットデータを暗号化して記録されたトラックと、暗号化しないで記録したトラックとが混在するテープの場合にも、検出が可能となる。

【００８６】また、あらかじめ記録されているソフトテープについても、以上説明した方法で、ソフトテープの作成および再生が可能となり、テープ上のパケットデータの保護が実現できる。

【００８７】以上は、記録トラックに現在のブロック鍵が格納されている例を示したが、データ鍵の演算は、Ｃ２の一演算サイクル内で行わなければならない。Ｃ２の一演算サイクル内でデータ鍵の演算が間に合わない場合は、前述のように、記録トラック内に、現在のブロック鍵と、次のブロック鍵を記録しておくことで、あらかじめ、次のデータ鍵を求めておける。

【００８８】図２４は図１のディジタル信号記録再生装置２００の他の構成図である。同図中、１２１は、例えばＩＥＥＥ１３９４のような高速ディジタルバスインターフェース等のプロトコルを実現するディジタルインターフェース回路であり、入力されたパケットデータの時間間隔を維持しながら、高速にデータを伝送する機能を有する、１２２は、ディジタルインターフェースバスである。１２３は、ディジタルインターフェース１２２上を伝送されるディジタルデータを保護するための暗号／復号回路であり、パケットデータを暗号化してディジタルインターフェースバス１２２上に伝送し、あるいは受信したディジタルデータを復号化する。１２４は、マイクロプロセッサのような制御回路であり、ディジタルインターフェース回路１２１、暗号／復号回路１２３を制御する。

【００８９】記録時には、ディジタルインターフェースバス１２２上を伝送されてきた暗号化されたディジタルデータをディジタルインターフェース回路１２１において、所定のパケット処理を行い、暗号／復号回路１２３において、元のパケットデータに復号して、入出力回路１０７に出力する。その後、前述で説明したように、データ暗号回路１１５でパケットデータを暗号化し、テープ１１１上に記録する。再生時には、データ復号回路１１６において、再生したパケットデータを復号化して、入出力回路１０７から暗号／復号回路１２３に出力し、暗号／復号回路１２３において暗号化して、ディジタル

インターフェース回路１２１から、ディジタルインターフェースバス１２２に出力する。これによれば、テープ上のパケットデータ、ディジタルインターフェースバス上のパケットデータの双方の保護が実現できる。

【００９０】次に、光ディスクでの実施例を説明する。

【００９１】図２５は、ディスク上に記録されているファイルの構成図である。６０１はリードイン領域であり、各種パラメータが格納されている。６０２、６０３、…は、プログラム１領域、プログラム２領域、…であり、各プログラム領域には、それぞれ異なる番組等が格納されている。

【００９２】図２６は、一つのプログラム領域例えばプログラム１領域の構成図である。プログラム領域は複数のユニットで構成され、この各ユニットに、例えば、後述するディジタル圧縮映像信号の一つの単位であるシーケンスを一個格納する。

【００９３】図２７は、ディジタル圧縮映像信号のフレーム単位で圧縮されたイントラフレームデータと、前後のフレームのデータよりの予測を用いて差分情報のみの圧縮を行ったインターフレームデータの関係である。６２１はイントラフレーム、６２２はインターフレームである。ディジタル圧縮映像信号は、所定数のフレーム、例えば１５フレームを一つのシーケンスとし、その先頭はイントラフレーム６２１とし、残りのフレームはイントラフレーム６２１からの予測を用いて圧縮したインターフレーム６２２としている。もちろん、先頭以外にもイントラフレーム６２１を配置するようにしてもよい。

【００９４】図２８は、ディジタル圧縮映像信号の構成である。６２３はフレーム単位で付加されるピクチャヘッダ、６２４はシーケンス単位で付加されるシーケンスヘッダである。シーケンスヘッダ６２４は、同期信号及び伝送レート等の情報により構成される。ピクチャヘッダ６２３は、同期信号及びイントラフレームかインターフレームかの識別情報等により構成される。通常、各データの長さは情報量により変化する。前述の一つのユニットに１シーケンスが格納される。

【００９５】前述図２６の各ユニットは、複数のデータセクタにより構成される。

【００９６】図２９は各データセクタの構成図である。６３１はＩＤ情報で4バイト、６３２はＩＤ情報６３１の誤り検出訂正のためのパリティで2バイト、６３３は管理データで6バイト、６３４はユーザデータで２０４８バイト、６３５はユーザデータ６３４の誤り検出訂正のためのパリティで4バイトから構成される。このうちユーザーデータ６３４に、図２８で示したディジタル圧縮映像信号が、分割され格納される。その他、ディジタル圧縮音声圧縮信号も、分割されユーザーデータ６３４に格納される。前述の一つのユニットは、ディジタル圧縮映像信号、音声信号が、それぞれ格納されたデータセクタの集まりである。

【００９７】図３０は、ディスクにデータセクタを記録する際に付加する誤り訂正符号を付加した構成図である。まず、データセクタが１７２バイトに区切られ、それに対し、１０バイトの第１の誤り検出訂正のためのパリティ６３７の一部（Ｃ１パリティパリティ６３７の一部）が付加される。さらにこのデータセクタをｎ個（例えば本実施例では１６個）集め、今度は行方向の１９２バイトに１６個の第２の誤り検出訂正のためのパリティ６３６（Ｃ２パリティ６３６）が付加される。得られたＣ２パリティ６３６にも１０バイトのＣ１パリティ６３７の一部が付加される。

【００９８】図３１は、光ディスクを記録媒体として用いたディジタル信号記録再生装置の構成図である。同図中、７０１は光ディスク、７０２は光ピックアップ、７０３ａは記録時の記録信号の生成等を行う記録信号処理回路、７０３ｂは再生時の再生信号の復調等を行う再生信号処理回路、７０４はマイクロプロセッサのような制御回路、７０５はスピンドルモータ、７０６は光ディスク７０１の回転速度および光ピックアップ７０２の位置、焦点を制御するサーボ回路、７０９は図６と同様の項構成のディジタル信号記録時のデータ暗号回路、７１０は図１９と同様の構成のディジタル信号再生時のデータ復号回路、７１１は、ディジタル信号を暗号あるいは復号する際にデータ暗号回路７０９あるいはデータ復号回路７１０に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、７１２はディジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるディスク鍵を発生するディスク鍵発生器、７１３はディジタル情報を暗号あるいは復号する際のデータ鍵のさらにもう一つのもとであるブロック鍵を発生するブロック鍵発生器、７１９はディジタルインターフェース回路、７２０は入出力端子である。

【００９９】記録時には、入出力端子７２０から、図２９のデータセクタのユーザデータ６３４の形式に区切られたディジタル圧縮映像信号等のディジタル信号が、ディジタルインタフェース回路７１９に入力される。入力されたディジタル信号は、データ暗号回路７０９において、デバイス鍵発生器７１１、ディスク鍵発生器７１２およびブロック鍵発生器７１３により発生される鍵をもとに制御回路７０４において生成されるデータ鍵によって、入力されたディジタル信号を暗号化し、これを記録信号処理回路７０３ａに出力する。記録信号処理回路７０３ａでは、入力されたユーザデータ形式のディジタル信号に、図２９のＩＤ６３１、パリティ６３２、管理データ６３３、およびパリティ６３５を付加し、データセクタの形式にする。次に、ｎ個のデータセクタを単位として（本実施例では１６個）、図３０のＣ１パリティ６３７、Ｃ２パリティ６３６を付加し、さらに図示しないが、所定の並べ替え、ヘッダを付加し、変調処理が施され、光ピックアップ７０２を介して光ディスク７０１上

に記録される。

【０１００】図３２は、データ暗号回路７０９に供給するデータ鍵の生成例であり、例えば、これらの生成は、図３１の制御回路７０４内にて行われる。デバイス鍵発生器７１１は、例えば９６ビットのあらかじめ定められた固定の鍵情報を記憶している。ディスク鍵発生器７１２、ブロック鍵発生器７１３は、例えば図３１の制御回路７０４からの司令７１２１、７１３１により９６ビットの乱数を発生させる乱数発生器である。７２１、７２２は９６ビットの排他的論理和演算器、７２３はハッシュ関数演算器である。まず、ブロック鍵は、ハッシュ関数演算器７２３にてハッシュ演算がなされ、その結果のうちの５６ビットが、データ鍵として図３１のデータ暗号回路７０９に供給される。また、９６ビットのブロック鍵は、９６ビットのディスク鍵と排他的論理和演算器７２２にて排他的論理和がとられ（以下鍵情報Ｋｒという）、図３１の記録信号処理回路７０３ａに送られ、光ディスク７０１上に記録される。さらに、ディスク鍵とデバイス鍵とが排他的論理和演算器７２１で排他的論理和がとられ（以下鍵情報ｋｄという）、図３１の記録信号処理回路７０３ａに送られ、光ピックアップ７０２を介して、光ディスク７０１上に記録される。

【０１０１】ここで、図３１の制御回路７０４からの司令７１３１を、ある時間間隔で発生させ、上述の演算によるデータ鍵の生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、光ディスク上のデータの安全性を高めることが可能となる。また、司令７１２１は、例えば一回の記録動作の際に一回発生させる。あるいは、空の光ディスクに最初に記録する際に一回だけ発生させてｋｄを記録し、次の記録動作からは、一旦光ディスク上の前述の鍵情報ｋｄを再生し、デバイス鍵と排他的論理和をとることで得られるディスク鍵を用いてブロック鍵と排他的論理和をとり鍵情報ｋｒを得る方法もある。さらに、ディスク鍵発生器７１２を用いずに、光ディスクの製造過程であらかじめ鍵情報ｋｄを記録しておき、記録動作の前にそのｋｄを再生し、ディスク鍵を得るという方法もある。鍵情報ｋｄは、例えば図２５のリードイン領域６０１に記録される。

【０１０２】再生の際には、まず鍵情報ｋｄを再生し、鍵情報ｋｄとデバイス鍵とを排他的論理和をとることでディスク鍵を得、さらに再生した鍵情報ｋｒと、得られたディスク鍵とを排他的論理和をとってブロック鍵を得、ハッシュ関数７２３の演算を行うことで、図３１のデータ復号回路７１０に入力するデータ鍵を得る。

【０１０３】図３１において、再生の際には、光ピックアップ７０２より再生された再生信号が再生信号処理回路７０３ｂに入力され、再生信号処理回路７０３ｂにおいて復調及び誤り検出訂正を行うとともに、図２９のユーザデータ６３４の形式のディジタル信号が、データ復号回路７１０に出力される。再生信号処理回路７０３ｂではディスク鍵、ブロック鍵情報の再生も行い、制御回路７０４に送る。、制御回路７０４においては、前述のデータ鍵再生の演算を行ってデータ復号回路７１０に供給する。データ復号回路７１０において再生信号処理回路７０３ｂからのディジタル信号が復号され、ディジタルインターフェース回路７１９を介して入出力端子７２０から出力される。

【０１０４】なお、記録するディジタル信号を保護する必要がない場合は、暗号化しないでそのまま光ディスクに記録してもよい。

【０１０５】図３３は、図２９の管理データ６３３の構成図である。この管理データ６３３に、前述の鍵情報ｋｒを格納する。６３４１はこの管理データ６３３が格納されているデータセクタのユーザデータが暗号化されているかどうかを示す暗号フラグ、６３４２はこの管理データに格納されている鍵情報が有効か無効かを示すデータ有効フラグ、６３４３は鍵情報ｋｒが一つの管理データ６３３に格納できない場合、後続の管理データがあることを示す鍵シーケンス番号、６３４４は鍵情報ｋｒである。

【０１０６】図３４は、鍵情報ｋｒを図２９の管理データ６３３の領域に格納する方法を示す図である。この例では、図３０のＣ２パリティ６３６の付加単位である１６個のデータセクタ（データセクタ０～データセクタ０１５）の管理データを一つの単位として、前述の６４ビットの鍵情報を格納する。９６ビットの鍵情報ｋｒは３個の管理データにｋｒ０、ｋｒ１、ｋｒ２に分割され格納される。その際、暗号フラグ６３４１は暗号化されていることを示す１″が、データ有効フラグは有効であることを示す“１”が、また、鍵シーケンス番号６３４３は、３個の管理データに順に２、１、０を格納し、０が分割の最後であることを示す。これらが、１６個の管理データに繰り返し格納される。ただし、最後の管理データは、半端となるので、データ有効フラグは無効であることを示す“０”が、格納される。

【０１０７】以上のように、鍵情報が光ディスク上に記録される。この時、鍵情報は１６個またはその整数倍のデータセクタを単位として更新される。この鍵情報の更新は、６４データセクタ、１２８データセクタ等、ｍ×ｎデータセクタ毎（ｍは１以上の整数、ｎは本実施例では１６）等に行うことが考えられるが、鍵の切り換わり目、あるいは暗号化の有無の境目は、Ｃ２パリティの付加単位（本実施例では１６データセクタ）の区切り目である。このことにより、再生時にＣ２パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【０１０８】なお、記録信号処理回路７０３ａ、再生信号処理回路７０３ｂは、図２０のディジタル記録再生信号処理回路１０２の動作と同様の動作を行う。ただし、Ｃ２パリティの付加単位は、ｎデータセクタ単位（本実施例では１６データセクタ）となる。

【０１０９】図３５は、光ディスクを記録媒体として用いたディジタル信号記録再生装置の他の構成図である。本実施例では、図３に示したディジタル映像圧縮信号の固定長のパケットを光ディスク７０１に記録再生する場合の例である。図３５中、７１７は、例えばＩＥＥＥ１３９４のような高速ディジタルバスインターフェース等のプロトコルを実現するディジタルインターフェース回路であり、入力されたパケットデータの時間間隔を維持しながら、高速にデータを伝送する機能を有する。７１８は、ディジタルインターフェースバスである。７１５はディジタルインターフェース７１８上を伝送されるディジタルデータを保護するための暗号／復号回路であり、パケットデータを暗号化してディジタルインターフェースバス７１８上に伝送し、あるいは受信したディジタルデータを復号化する。７１６は、マイクロプロセッサのような制御回路であり、ディジタルインターフェース回路７１７、暗号／復号回路７１５を制御する。７０７はパケットデータをデータセクタのユーザデータに変換、あるいはユーザデータからパケットデータを取り出すセクタ変換回路、７０８は記録時のパケットデータへのタイムスタンプ処理、再生時のパケットデータの出力制御を行う入出力制御回路である。

【０１１０】記録時には、ディジタルインターフェース回路７１７において、ディジタルインターフェースバス７１８上を伝送されてきた暗号化されたディジタルデータに所定のパケット処理を行い、暗号／復号回路７１５において、元のパケットデータに復号して、入出力回路７１４に出力する。その後、データ暗号回路７０９でパケットデータを暗号化し、入出力制御回路７０８において入力されたパケットデータにタイムスタンプを施し、セクタ変換回路７０７に出力する。セクタ変換回路７０７では、入力されたパケットデータを前述のデータセクタのユーザデータの形式に変換する。ユーザデータの形式に変換されたディジタル信号が、記録信号処理回路７０３ａ及び光ピックアップ７０２を介して、光ディスク７０１上に記録される。

【０１１１】したがって、光ディスク７０１上には、鍵情報に所定の演算を行って得られた鍵で暗号化された前記ディジタル信号と共に、前記鍵情報が、所定の領域に記録されている。また前記ディジタル信号は、所定長のパケット形式を有してなる。さらに、前記鍵情報が所定間隔で更新され、所定の領域に記録されている。またさらに、複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録されている。

【０１１２】再生時には、光ピックアップ７０２及び記録信号処理回路７０３ａを介して、セクタ変換回路７０７において、再生したユーザデータからパケットデータを取り出し、入出力制御回路７０８において記録時に付加されたタイムスタンプをもとに出力タイミングを制御しタイムスタンプが取り除かれたパケットデータが出力される。さらに、データ復号回路７１０において、再生したパケットデータを復号化して、入出力回路７１４から暗号／復号回路７１５に出力し、暗号／復号回路７１５において暗号化して、ディジタルインターフェース回路７１７から、ディジタルインターフェースバス７１８に出力する。

【０１１３】図３６は、図３５のセクタ変換回路７０７によって変換された図２９のデータセクタのユーザデータ６３４に格納されるパケットデータの構成図である。ディジタル映像圧縮信号の固定長のパケットが複数個格納される。図３５の入出力制御回路７０８において、各パケット６４３，６４５、…には、例えば４バイトの時間情報６４２，６４４、…が付加される。データセクタが２０４８バイトの場合、時間情報が付加された１０個のパケットが格納可能である。時間情報が付加されたパケットは、連続して格納される必要はなく、途中に未使用領域があってもよい。また、パケットヘッダ６４１を付加することで、パケットの区切り目を容易に判別することができる。

【０１１４】本実施例においても、前述の鍵情報を切り換えるタイミング、あるいは暗号化の有無の境目としては、このＣ２パリティの付加単位であるｎデータセクタ（本実施例では１６データセクタ）の区切り目とすることで、再生時にＣ２パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【０１１５】図３７は、図３６の各時間情報６４２，６４４、…の構成図である。暗号フラグ６５１は、パケットが暗号化されているかどうかを示すフラグであり、鍵フラグは、このパケットが暗号化されている場合、どの鍵で暗号化されているかを示すフラグである。例えば、このフラグを２ビットとして、鍵が更新される度に０、１、２、３と１ずつ増加する値をとり、同様のフラグを図２９の管理データにも格納しておくことで、各パケット毎に対応する鍵を明示することができる。これらのフラグは、前述のパケットヘッダ６４１に格納してもよい。この方法によれば、パケット毎に任意に鍵を更新することが可能となる。

【０１１６】なお、以上の実施例では、磁気テープおよび光ディスクでの記録再生について説明したが、磁気ディスクや、半導体メモリ等、他のあらゆる記録媒体に記録再生する場合でも、同様に適用することができる。

【０１１７】上記半導体メモリの場合には、鍵情報の切り換え、あるいは暗号化するかしないかの切り換えは、例えば半導体メモリの記録の一つの単位であるアドレスの区切り目で行うとよい。

【０１１８】また、本実施例は、本発明を、ディジタル信号を鍵により暗号化するシステムに適用したものである。しかし、本発明はこの実施例に限定されるものではなく、例えば、ディジタル信号がキーコードによりスクランブルされたりするシステムにも適用可能である。す

なわち、本発明は、少なくとも、ディジタル信号が元々のクリアな状態から変換されるように処理されるあらゆるシステムに対して適用可能なものである。

【０１１９】

【発明の効果】本発明によれば、ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力する。以上により、再生の際には、前記所定の演算を施さない限り、前記鍵が得られないので、記録媒体上の鍵情報を得ても、それを用いて暗号化されたディジタル信号を復号することは困難であり、記録媒体上のディジタル信号の著作権を保護することができる。

【図面の簡単な説明】

【図１】本発明の実施例で、ディジタル放送受信機とディジタル信号記録再生装置を含む構成図である。

【図２】図１のディジタル信号記録再生装置２００の構成図である。

【図３】ディジタル映像圧縮信号のパケットの構成図である。

【図４】図３のパケットヘッダ３０６の構成図である。

【図５】ディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。

【図６】図２のデータ暗号回路１１５の構成図である。

【図７】図６の暗号器１１５５の構成図である。

【図８】図２のデータ暗号回路１１５、データ復号回路１１６に供給するデータ鍵の生成例を示すところの制御回路１０４内のデータ鍵の生成図である。

【図９】テープ１１１の１トラックの記録パターンを示す図である。

【図１０】図９のデータ記録領域７のブロックの構成図である。

【図１１】図１０のＩＤ情報２１の構成図である。

【図１２】図９のデータ記録領域７の１トラック分のデータの構成図である。

【図１３】１８８バイトのパケット形式で伝送されたディジタル圧縮映像信号を、図１２のデータ４１に記録する時の１パケットのブロックの構成図である。

【図１４】図１２のデータ記録領域７のヘッダ４４の構成図である。

【図１５】図１４の付加情報４７の領域に、ブロック鍵を格納する場合のパックデータの構成図である。

【図１６】ブロック鍵の格納方法を示す図である。

【図１７】ブロック鍵の他の格納方法を示す図である。

【図１８】図１３の時間情報２５の具体的構成図である。

【図１９】図２のデータ復号回路１１６の構成図である。

【図２０】図２の記録信号処理回路１０２ａおよび再生信号処理回路１０２ｂからなるディジタル記録再生信号処理回路１０２の構成図である。

【図２１】データ記録開始時における信号処理のタイミングを示す図である。

【図２２】図２のテープ１１１上の鍵情報を示す図である。

【図２３】データ再生時における信号処理のタイミングを示す図である。

【図２４】図１のディジタル信号記録再生装置２００の他の構成図である。

【図２５】ディスク上に記録されているファイルの構成図である。

【図２６】一つのプログラム領域の構成図である。

【図２７】ディジタル圧縮映像信号のイントラフレームデータとインターフレームデータの関係を示す図である。

【図２８】ディジタル圧縮映像信号の構成図である。

【図２９】データセクタの構成図である。

【図３０】ディスクにデータセクタを記録する際に付加する誤り訂正符号を付加した構成図である。

【図３１】光ディスクを記録媒体として用いたディジタル信号記録再生装置の構成図である。

【図３２】データ暗号回路７０９に供給するデータ鍵の生成例を示す図である。

【図３３】図２９の管理データ６３３の構成図である。

【図３４】鍵情報ｋｒを管理データ領域に格納する方法を示す図である。

【図３５】光ディスクを記録媒体として用いたディジタル信号記録再生装置の他の構成図である。

【図３６】図２９のデータセクタのユーザデータ６３４に格納されるパケットデータの構成図である。

【図３７】暗号フラグ等を前述の時間情報に付加する場合の時間情報の構成図である。

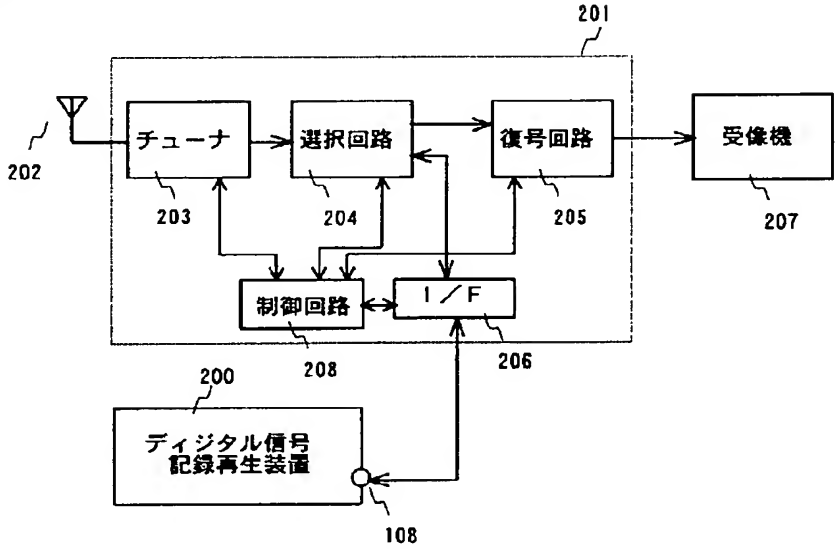
【符号の説明】

７…データ記録領域、２０…同期信号、２１…ＩＤ情報、２２…データ、２５…時間情報、３１…グループ番号、３２…トラックアドレス、３３…ブロックアドレス、４１…映像信号データ、４４…ヘッダ、４５…フォーマット情報、４６…ブロック情報、４７…付加情報、７１…パケット、１００…回転ヘッド、１０１…キャプスタン、１０２ａ…記録信号処理回路、１０２ｂ…再生信号処理回路、１０４…制御回路、１０５…タイミング生成回路、１０６…サーボ回路、１０７…入出力回路、１０９…タイミング制御回路、１１０…発振回路、１１５…データ暗号回路、１１６…データ復号回路、１１７…デバイス鍵発生器、１１８…ブロック鍵発生器、１１９…入出力制御回路、２００…ディジタル信号記録再生

装置、２０１…ディジタル放送受信機、２０３…チューナ、２０４…選択回路、２０５…復号回路、２０６…インターフェース回路、２０８…制御回路、１１５２…ブロック処理回路、１１５４…鍵スケジュール回路、１１５５…暗号器、１１５８…データ鍵レジスタ、１１５９…データ鍵セレクタ、１１６５…復号器、４００…メモリ回路、４０１…メモリ制御回路、４０２…Ｃ２パリティ演算回路、４０３…Ｃ１パリティ演算回路、４０４…付加情報処理回路、４０５…変復調回路、５５１…暗号処理部。７０１…光ディスク、７０２…光ピックアップ、７０３ａ…記録信号処理回路、７０３ｂ…再生信号処理回路、７０４…制御回路、７０５…スピンドルモータ、７０６…サーボ回路、７０７…セクタ変換回路、７０８…入出力制御回路、７０９…データ暗号回路、７１０…データ復号回路、７１１…デバイス鍵発生器、７１２…ディスク鍵発生器、７１３…ブロック鍵発生器、７１９…ディジタルインターフェース回路。

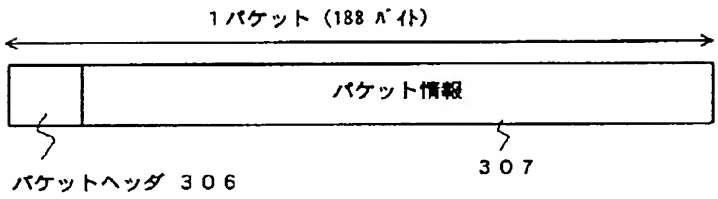
【図１】

図１



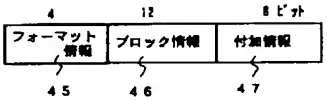
【図３】

図３



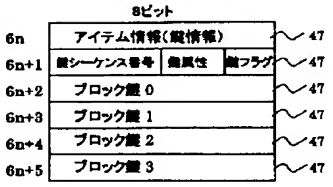
【図１４】

図１４



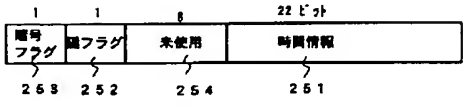
【図１５】

図１５



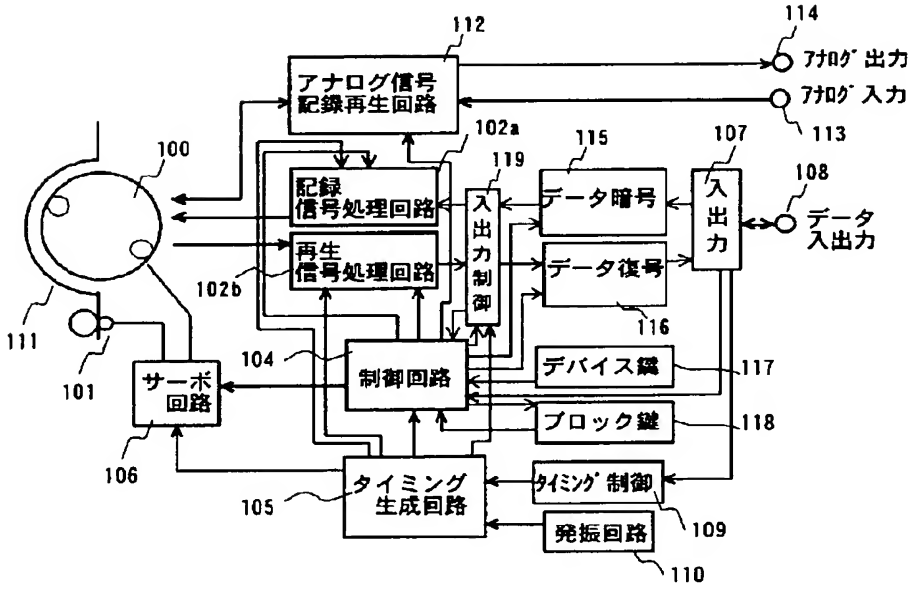
【図１８】

図１８



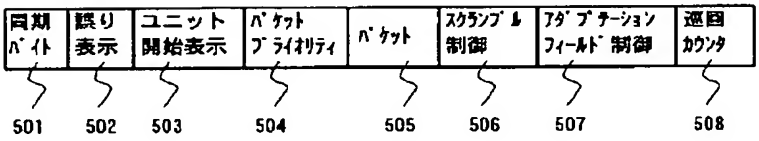
【図２】

図２



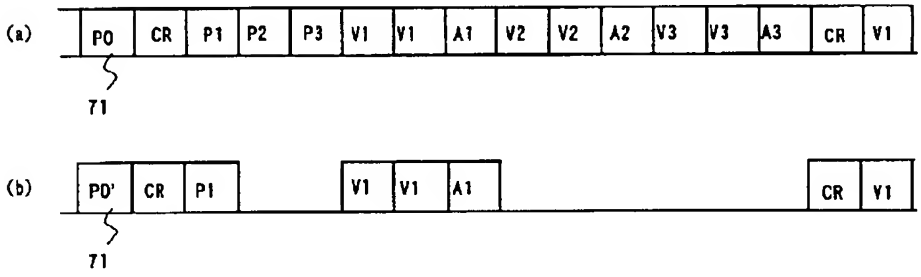
【図４】

図４



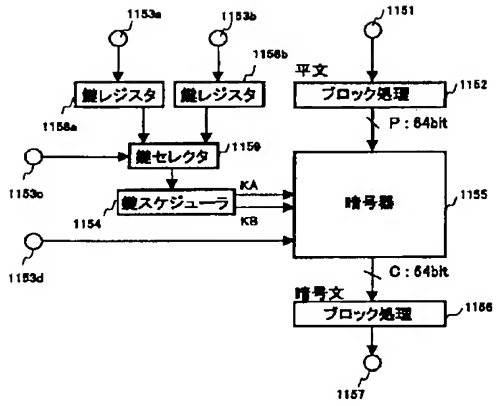
【図５】

図５



【図６】

図６

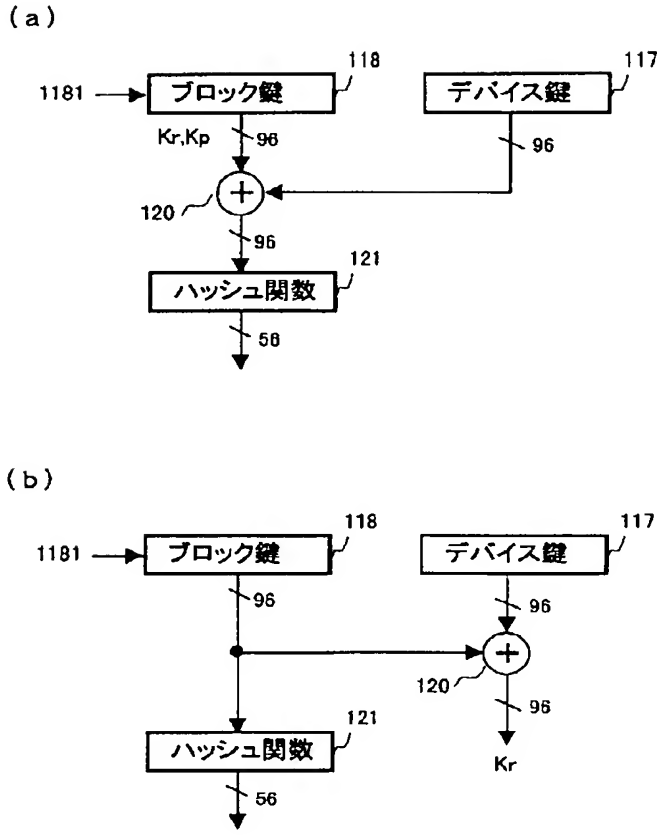


【図２５】

図２５

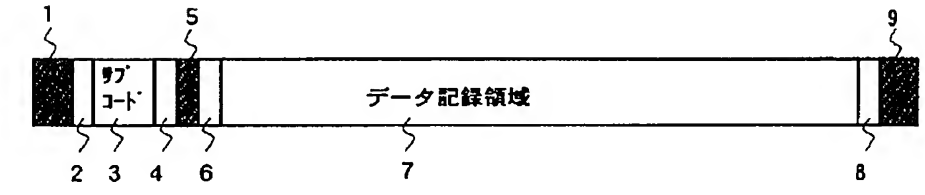
【図８】

図８



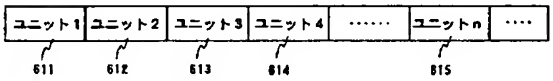
【図９】

図９



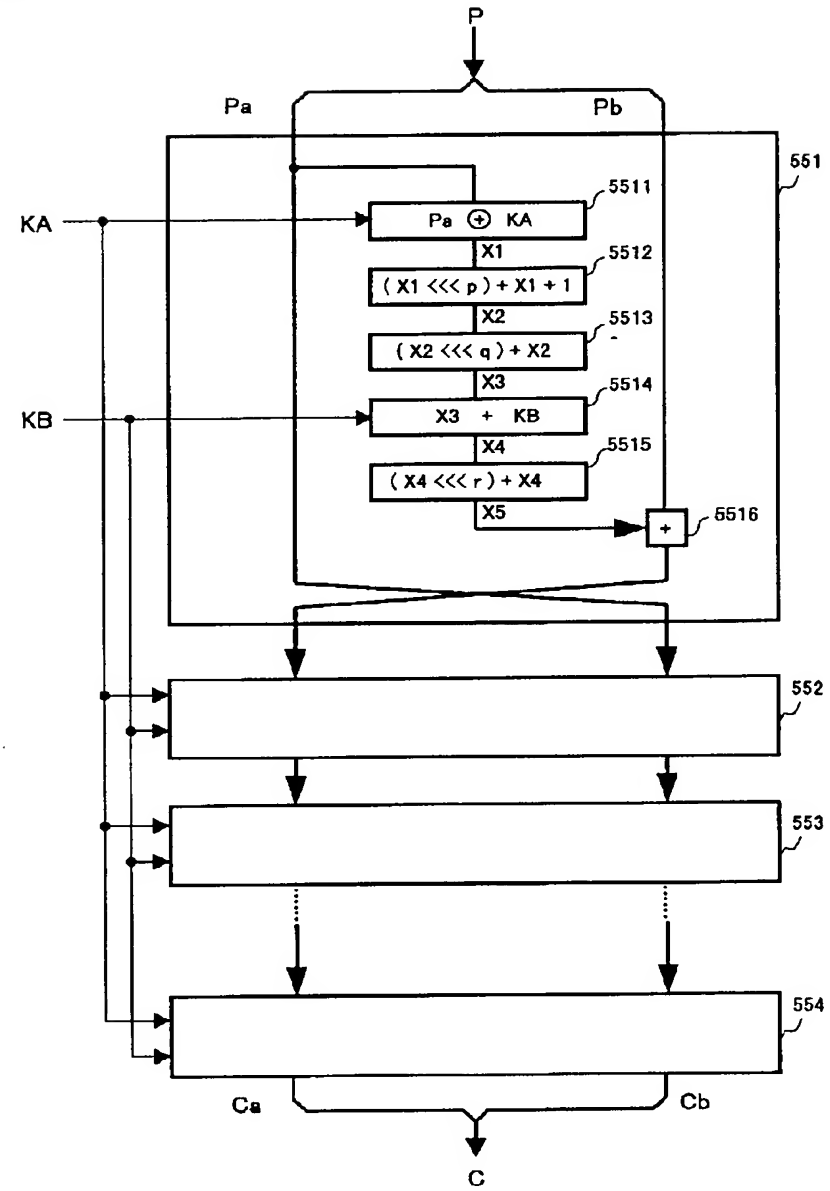
【図２６】

図２６



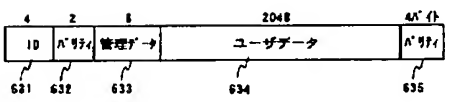
【図７】

図７



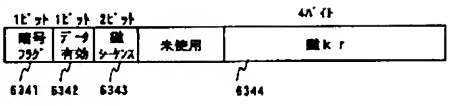
【図２９】

図２９



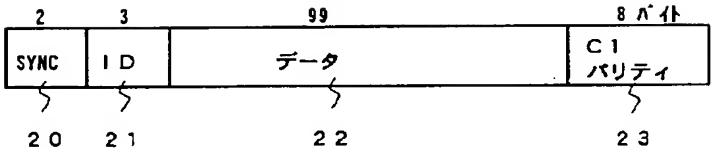
【図３３】

図３３



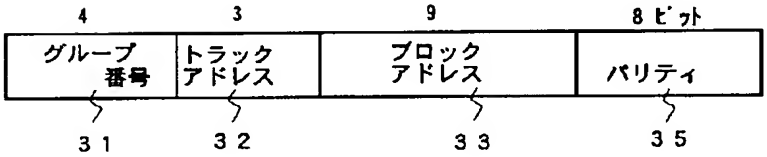
【図１０】

図１０



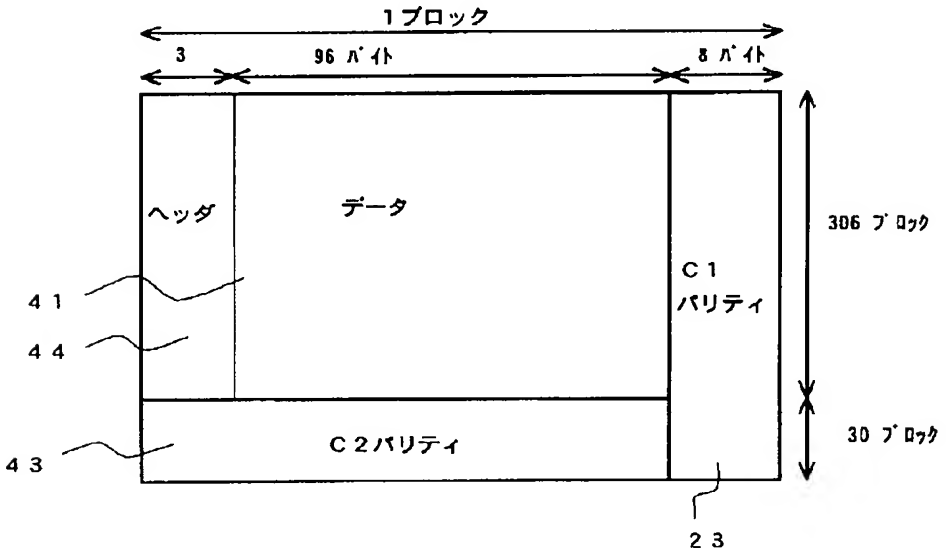
【図１１】

図１１



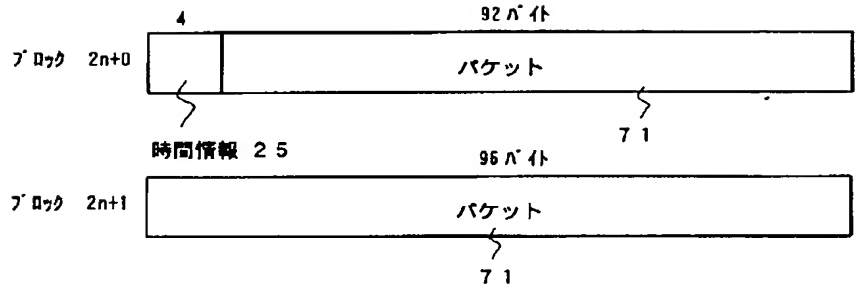
【図１２】

図１２



【図１３】

図１３



【図１６】

図１６

(1)

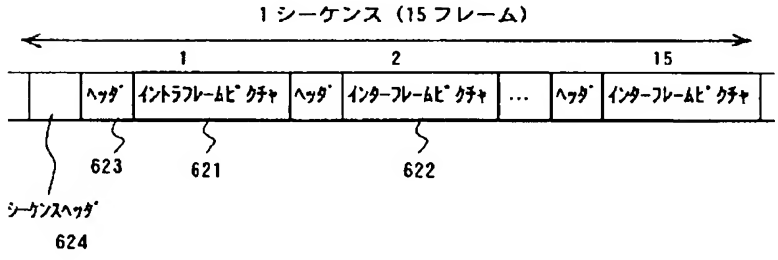
6a	“鍵情報”			6b	“鍵情報”			6c	“鍵情報”		
6a+1	“2”	“0”	“0”	6b+1	“1”	“0”	“0”	6c+1	“0”	“0”	“0”
6a+2	ブロック鍵 A0			6b+2	ブロック鍵 A4			6c+2	ブロック鍵 A8		
6a+3	ブロック鍵 A1			6b+3	ブロック鍵 A5			6c+3	ブロック鍵 A9		
6a+4	ブロック鍵 A2			6b+4	ブロック鍵 A6			6c+4	ブロック鍵 A10		
6a+5	ブロック鍵 A3			6b+5	ブロック鍵 A7			6c+5	ブロック鍵 A11		

(2)

6d	“鍵情報”			6e	“鍵情報”			6f	“鍵情報”		
6d+1	“2”	“0”	“1”	6e+1	“1”	“0”	“1”	6f+1	“0”	“0”	“1”
6d+2	ブロック鍵 B0			6e+2	ブロック鍵 B4			6f+2	ブロック鍵 B8		
6d+3	ブロック鍵 B1			6e+3	ブロック鍵 B5			6f+3	ブロック鍵 B9		
6d+4	ブロック鍵 B2			6e+4	ブロック鍵 B6			6f+4	ブロック鍵 B10		
6d+5	ブロック鍵 B3			6e+5	ブロック鍵 B7			6f+5	ブロック鍵 B11		

【図２８】

図２８



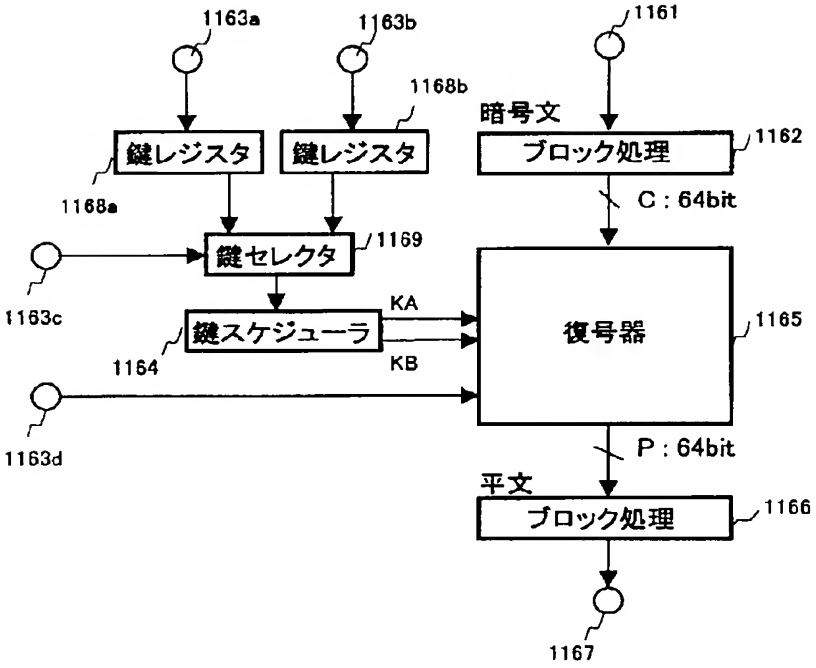
【図１７】

図１７


(1)
6a "鍵情報" "2" "0" "0" ブロック鍵 A0 ブロック鍵 A1 ブロック鍵 A2 ブロック鍵 A3
6b "鍵情報" "1" "0" "0" ブロック鍵 A4 ブロック鍵 A5 ブロック鍵 A6 ブロック鍵 A7
6c "鍵情報" "0" "0" "0" ブロック鍵 A8 ブロック鍵 A9 ブロック鍵 A10 ブロック鍵 A11
(2)
6d "鍵情報" "2" "1" "1" ブロック鍵 B0 ブロック鍵 B1 ブロック鍵 B2 ブロック鍵 B3
6e "鍵情報" "1" "1" "1" ブロック鍵 B4 ブロック鍵 B5 ブロック鍵 B6 ブロック鍵 B7
6f "鍵情報" "0" "1" "1" ブロック鍵 B8 ブロック鍵 B9 ブロック鍵 B10 ブロック鍵 B11
(3)
6a "鍵情報" "2" "0" "1" ブロック鍵 B0 ブロック鍵 B1 ブロック鍵 B2 ブロック鍵 B3
6b "鍵情報" "1" "0" "1" ブロック鍵 B4 ブロック鍵 B5 ブロック鍵 B6 ブロック鍵 B7
6c "鍵情報" "0" "0" "1" ブロック鍵 B8 ブロック鍵 B9 ブロック鍵 B10 ブロック鍵 B11
(4)
6d "鍵情報" "2" "1" "0" ブロック鍵 C0 ブロック鍵 C1 ブロック鍵 C2 ブロック鍵 C3
6e "鍵情報" "1" "1" "0" ブロック鍵 C4 ブロック鍵 C5 ブロック鍵 C6 ブロック鍵 C7
6f "鍵情報" "0" "0" "0" ブロック鍵 C8 ブロック鍵 C9 ブロック鍵 C10 ブロック鍵 C11

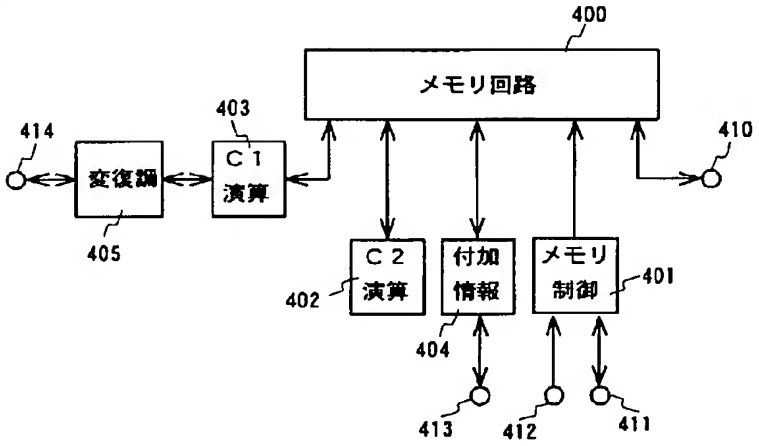
【図１９】

図１９



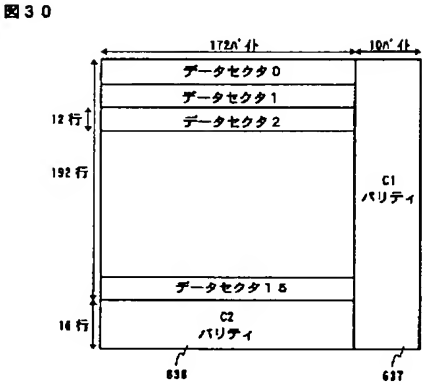
【図２０】

図２０



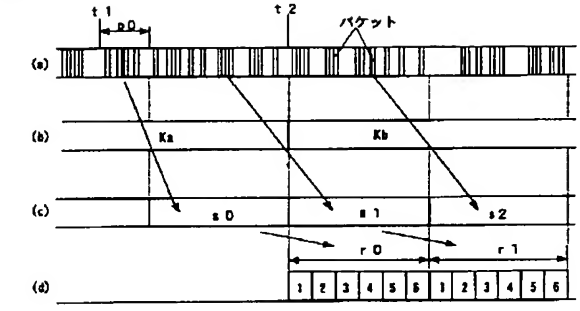
【図３０】

図３０



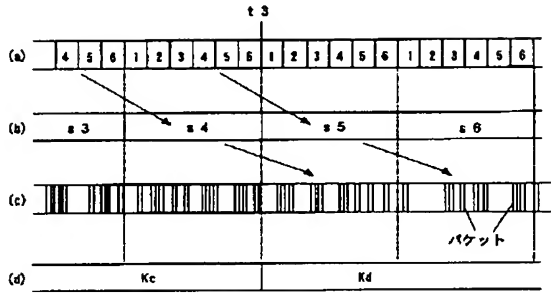
【図２１】

図２１



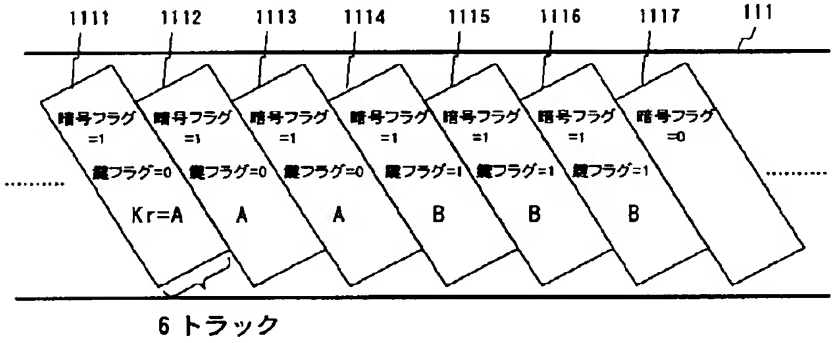
【図２３】

図２３



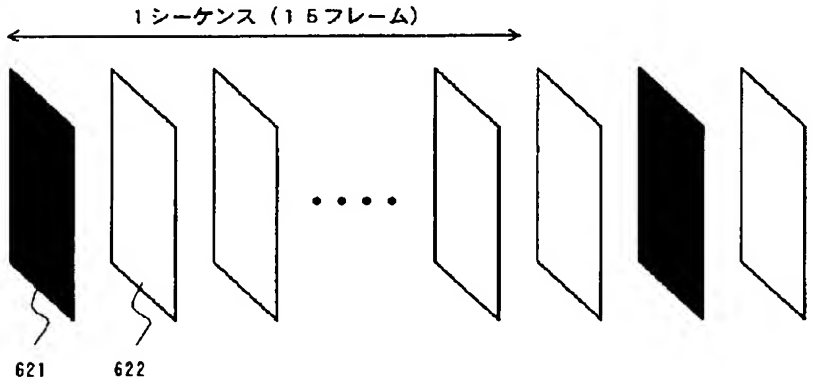
【図２２】

図２２



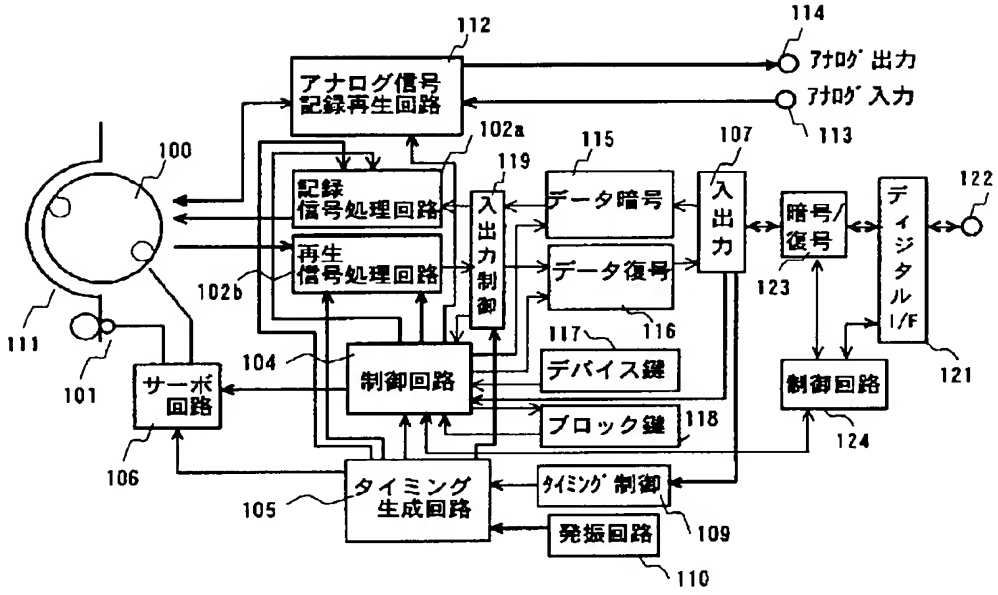
【図２７】

図２７



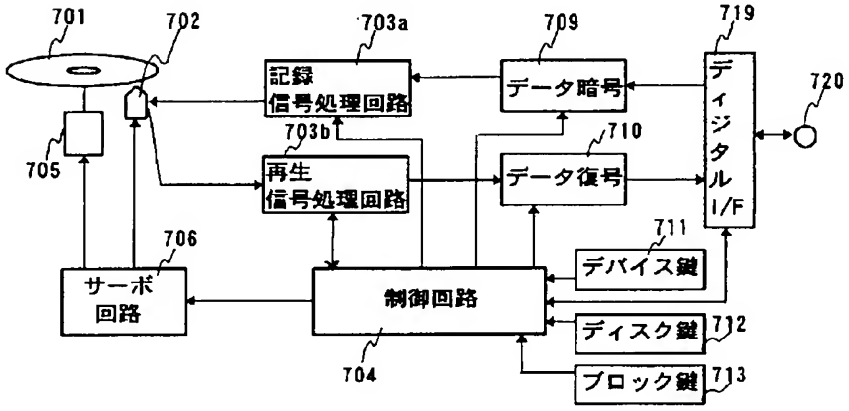
【図２４】

図２４



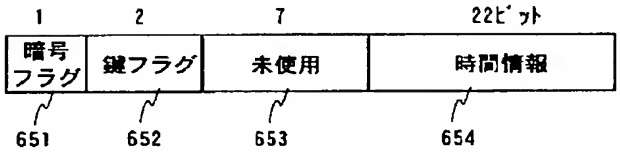
【図３１】

図３１



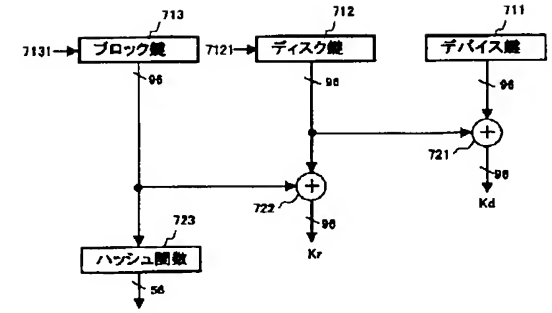
【図３７】

図３７



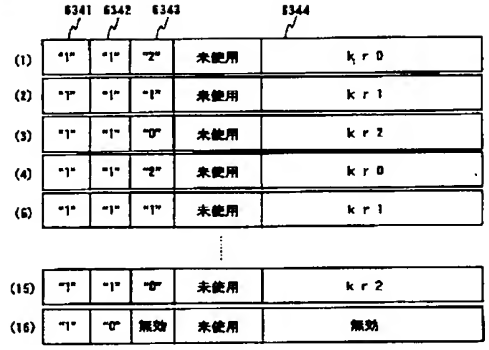
【図３２】

図３２



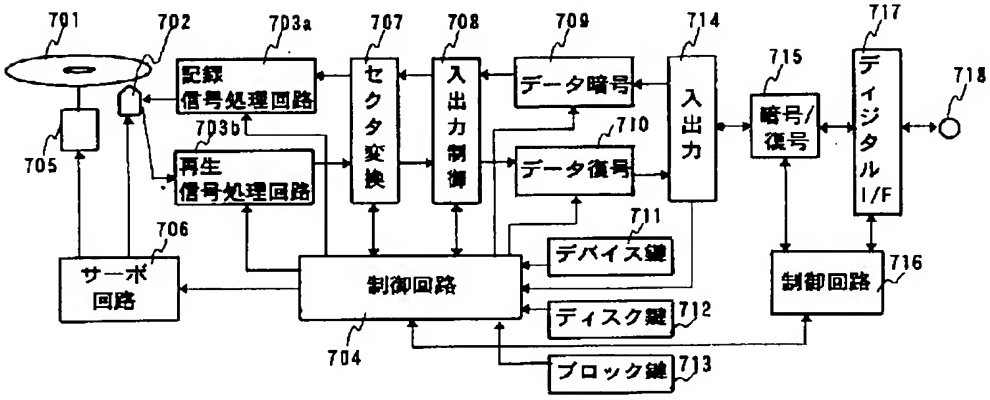
【図３４】

図３４



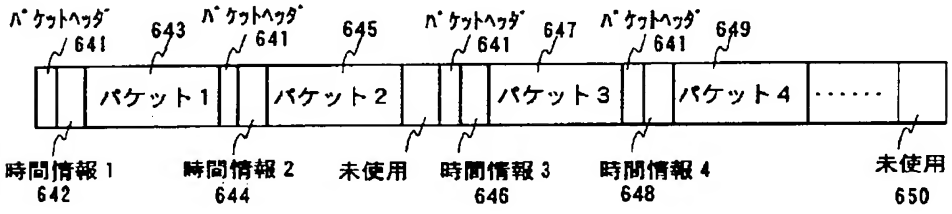
【図３５】

図３５



【図３６】

図３６



フロントページの続き

(72)発明者　千葉　浩
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　尾鷲　仁朗
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

Ｆターム(参考)　5C053 FA13 FA20 FA22 FA23 GB01 GB06 GB07 GB11 GB15 GB21 GB30 GB37 JA21 JA22 JA26 KA01 KA08 KA21 KA22 KA24 LA06 LA07
5D044 AB05 AB07 DE03 DE48 DE50 DE52 DE60 DE68 GK08 GK17